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

2023 Research Calendar

Table of Contents

Digital Service Execution

Valerie O'Connell

Automation, AI, and the Rise of ServiceOps

Q1 2023	AI-enabled automated actions and cross-functional processes blur the lines between IT service and IT operations in the drive for IT service excellence. This research examines how automation and AI/ML enable and shape a ServiceOps model of IT service delivery and support. It will look at ways that progressive organizations strike a balance between the specialization of advanced technologies and the commonalities of business innovation that digital transformation demands.

AIOps Major Trends 2023: A Hybrid View

Q2 2023	Part field research and part vendor review, this initiative will explore field-based perceptions, plans, and adoption of major AIOps trends. Vendors will be invited to sponsor an AIOps use case, area, or technology to be probed in targeted field research. EMA will combine the findings with the vendor solutions to provide IT executive and technical buyers with clear, practical understanding of the differing capabilities of key AIOps vendors, punctuated by field research. Participation in this hybrid, real-world view of AIOps will be limited in order to minimize competitive friction and functional overlap.

CMDB in Cloud Times

Q2 2023	Despite persistent trade press claims that cloud cuts CMDB relevance, EMA research consistently finds the opposite to be true. In a 2022 initiative, 400 global IT leaders stated that CMDB use was central to major functions. For 31% of the respondents, CMDB use was viewed as increasing in importance for automation of complex processes. However, nobody said it would be easy. This research will dive into the uses, challenges, technologies, and organizational structures that go into CMDB usefulness. With attention to discovery and dependency mapping, it will look at CMDB competency in the days of Kubernetes and everything cloud.

The Anatomy of Modern Incident Management

Q3 2023	When EMA recently asked 300 global IT leaders, "If you could choose one thing to do really well, what would have the biggest positive impact?" 60% chose proactive response to incidents before they become outages. AI/ML and automation hold great promise moving toward that goal, yet users still report 30% of all service problems. What are the causes and practical cures for that gap? This research takes an enterprise-wide view of incident management, from mean time to detect to the many meanings of "R" in MTTR. Special attention will be paid to technologies, practices, and organizational changes that are making a difference today.

Digital Service Execution

Valerie O'Connell

Optimizing IT Service for Business Performance

Q4 2023	As digital transformation continues to compound complexity, scope, and speed of change, the need to view the IT estate in its business context is critical—but not simple. New technologies and capabilities challenge traditional answers to even basic questions, like "What is an asset?" The answers increasingly include new entries, like edge devices, industrial IoT, operational technology, and technologies in the clouds and across the globe. IT is being 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 and processes, and the functional organizations needed to align the interests and actions of IT and the business it serves.

Endpoint and Identity Management

Steve Brasen

Orchestrating Positive Customer Experiences with Consumer Identity and Access Management (CIAM)

Q1 2023	While CIAM solutions are most frequently adopted to help organizations meet security and compliance requirements, their employment has a direct impact on the experiences of all consumers involved in digital engagements. Access processes are instrumental in forming the first impressions consumers will have with a business's brand, products, and services, and that perspective will be reinforced during each and every future engagement. Consumer experiences are impacted by the types of adopted CIAM-specific processes and solutions, including for low-friction authentication, self-registration, privacy consent, credential resets, and progressive profiling orchestration. EMA will conduct primary, survey-based research to identify the types of approaches employed for each of these and quantify their value for attracting and retaining consumers of business IT services.

EMA Radar Report for Privileged Access Management (PAM)

Q2 2023	According to EMA primary research, roughly 25% of business workers retain privileged access to enterprise devices, applications, and servers. The methods for controlling access to organizations' most sensitive data and IT services is most effectively achieved with the adoption of a privileged access management (PAM) platform. To help provide purchasing guidance on the optimal PAM solutions organizations should adopt to achieve their unique goals, EMA is performing an objective and independent evaluation of the leading PAM solutions. This market landscape report will clearly identify industry value leaders through careful analysis of the solutions' breadth of functionality, cost-effectiveness, architecture, integration, deployment, administration, and vendor strength. Value leaders and innovators will be recognized with awards.

Enhancing Unified Endpoint Management (UEM) by Gauging Digital Employee Experiences (DEX)

Q3 2023	Modern management theory states that workers are motivated more by job satisfaction than they are by monetary compensation. Maintaining a productive workforce—especially in a world where employees more frequently operate remotely from the physical office—requires endpoint management functionality that monitors and adapts to end-user preferences and unique requirements. DEX functionality that is being incorporated into traditional UEM platforms includes user sentiment surveys, real user monitoring (RUM), intelligent analysis of user experiences, the establishment of a standardized user experience score, and the automated remediation of user experience issues. In this survey-based research project, EMA will evaluate the workforce productivity improvements gained by the introduction of DEX functionality, as well as the enhancements achieved in attracting and retaining talent.

Endpoint and Identity Management

Steve Brasen

Transcending Passwords: The Next Generation of Authentication Methods

Q4 2023	The use of low-friction authentication alternatives to passwords—including security keys, biometrics, and behavioral analysis technologies—has been accelerating in recent years. Most recently, the introduction of passkeys promises to fulfill the long-held dream of eliminating passwords entirely. This EMA primary research project will evaluate the available passwordless approaches to offer guidance on their value to workforce productivity, security effectiveness, and optimal implementation. Additionally, the research will examine public sentiment and confidence levels with utilizing passwordless authentication methods. Also, business adoption rates with related solutions will be quantified and correlated with the introduction of industry standards, such as FIDO, SAML, and OAuth.

Intelligent Automation

Dan Twing

2023 Radar Report for Workload Automation

Q2 2023	The EMA Radar Report delivers an in-depth analysis of leading vendors and vendor products, including their overall market position in comparison with other vendors. This information is laid out in an easy-to-decipher, detailed market map and Radar Chart – which includes a composite score for each vendor – making it simple to see how vendors measure up in the market, as well as against other vendors. The EMA Radar Report also provides a detailed discussion of methodology and criteria, a high-level market segment overview, a comprehensive analyst writeup on each vendor, and more.

The Automation Destination: Enterprise Approaches and Tools for Automation Success

Q4 2023	Workload automation is transitioning from an IT operations tool to a more enterprise-wide orchestrator of automation. This research will extend the 2022 research, "From Scheduler to Automation Fabric for the Enterprise: Workload Automation Transformation in 2022" to assess the adoption of automation orchestration and the role of WLA in enterprise automation use cases. Much of EMA's prior research on WLA focused on those using WLA tools and those managing users of WLA tools. With this research, EMA will expand the focus to look at automation more generally, explore how enterprises approach automation projects, and identify other tools contending for the role of automation orchestrator.

Intelligent Hybrid Multi-Cloud

Torsten Volk

Five Best Practices for Optimizing the Business Value of Microservices

Q4 2022	When 1,500 applications turn into 20,000-30,000, microservices organizations experience a whole new set of pain points in app development, DevOps, security, site reliability engineering, and cloud engineering. This report will reveal the most important challenges, priorities, and trends experienced by each of these personas during the development lifecycle of distributed applications. Based on these real-world findings, the report will derive five critical best practices that enable the organization to maximize the business value of transitioning toward a microservices-centric application architecture.

Machine Learning on Kubernetes at Scale: Pain Points, Enterprise Priorities, and Success Factors

Q1 2023	The study will explore key requirements, adoption patterns, pain points, investment priorities, and success factors of deploying and operating machine learning models on Kubernetes. Readers will receive guidance related to existing and future applications that run within the corporate data center, the public cloud, at near-edge low-latency data centers, or at far-edge locations. EMA will identify the challenges and opportunities of enabling applications to analyze streaming real-time data and static transactional data in order to capture new business cases.

Code Once, Deploy Anywhere: Critical Steps Toward Maximizing Developer Productivity

Q1 2023	Software developers spend approximately 50% of their day on non-development-related tasks. Freeing up the "other 50%" of developer productivity would significantly increase an organization's ability to beat its competition by releasing better products faster and cheaper. This study will identify all non-development tasks that are part of a developer's day and determine a list of requirements for organizations to address or eliminate these tasks to unleash optimal developer productivity. Within this context, EMA will look into the importance of infrastructure as code, GitOps, MLOps, observability, automation, and machine learning to achieve this goal.

EMA Top 3 Product Guide: Developer Platforms for Maximum Productivity

Q1 2023	Fifty percent of app developer productivity remains untapped because developers spend half of their time on overhead tasks that are unrelated to writing business code. This EMA Top 3 Product Guide will identify the key factors that slow down software developers in 2023 in order to isolate the best three developer platforms for organizations to adopt, with the goal of maximizing the amount of time developers can spend on coding.

Intelligent Hybrid Multi-Cloud

Torsten Volk

The Five Best Practices for Cloud-Native Compliance

Q2 2023	Ninety-five percent of incidents that affect security and reliability are due to human error. This research report will reveal five best practices for creating automated compliance guardrails to achieve optimal flexibility and control for developing, deploying, running, and managing cloud-native applications within a brownfield enterprise context. All report findings will be based on the analysis of real-life data breaches and outages experienced by organizations over the previous 12 months.

EMA Top 3 Product Guide: Observability Platforms

Q2 2023	Over 300% growth of the market for observability platforms over the previous three years, combined with the fact that a lack of observability remains the number-one challenge for site reliability engineers (SRE), places the EMA Top 3 Product Guide for observability platforms near the top of our list of priorities. The guide will crown products that successfully leverage machine learning; simple and robust data collection methods; real-time analytics to enable developers, SREs, and DevOps engineers to receive a business-centric picture of application environments; and DevOps pipelines across data centers, clouds, and edge locations.

Data Analytics and Machine Learning for Everyone

Q2 2023	While machine learning is and has been one of the critical trends in business, most business staff are unable to leverage data analytics and machine learning capabilities to solve daily business challenges. This study will look at the potential business impact of "democratizing" machine learning at all levels of the business, corporate IT, and DevOps. EMA will identify the low-hanging fruit, the high-value targets, and everything in between to determine concrete steps for businesses to beat the competition through enabling machine learning-driven decision-making and automation everywhere. This report may include the introduction of tools and platforms for businesses to look at in order to accelerate their journey toward an AI-driven enterprise.

The Five Best Practices for AI and Machine Learning

Q3 2023	Data-driven decision-making and automation constitute the backbone of an organization's ability to successfully compete in the marketplace. This research report will analyze areas in which organizations already successfully leverage machine learning and AI, and identifies where they are still struggling. Based on a detailed analysis of pain points from the perspectives of software developers, business analysts, data engineers, data scientists, and IT operations engineers, this research will identify the five best practices for organizations to adopt in order to successfully widen the use of machine learning and AI technologies for maximum business impact.

EMA Top 3 Product Guide: AI and Machine Learning Platforms

Q3 2023	This EMA Top 3 Product Guide will be based on the empirical findings of its sister project, "The Five Best Practices for AI and Machine Learning" and will recommend the top three machine learning and AI platforms that best address current pain points of software developers, data scientists, data engineers, and IT operations engineers.

Intelligent Hybrid Multi-Cloud

Torsten Volk

Scaling Up MLOps – Accelerating Time to Value

Q3 2023	The study will identify critical gaps in an organization's ability to quickly and cost-effectively build, train, deploy, continuously enhance, and share machine learning models. EMA will attempt to quantify the gap between potentially viable machine learning use cases and the use cases that are feasible under an organization's current constraints. The analysis will look at all aspects of MLOps, including experimentation, training, tuning, pipeline building, infrastructure automation, data management, feature lifecycle management, use of purpose-built hardware, real-time data analysis, and numerous further potential factors. Finally, EMA will provide a checklist for enterprises to determine their own individual strengths and weaknesses.

EMA Top 3 Product Guide: Managed Kubernetes Platforms

Q4 2023	The rapid growth in Kubernetes adoption as the de facto standard platform for cloud-native applications has resulted in many enterprises struggling with optimally deploying, governing, and managing Kubernetes clusters within their data centers, on AWS, Azure, GCP, and at edge locations. This EMA Top 3 Product Guide will reveal the real-life pain points of Kubernetes operations and recommends three managed Kubernetes platforms that enable organizations to maximize developer productivity without sacrificing operational efficiency and compliance.

Unified Kubernetes Management for Policy-Driven Application Deployment and Day 2 Management in Data Centers, Public Cloud, and at the Edge

Q4 2023	The study will determine challenges, adoption patterns, priorities, and success factors related to managing Kubernetes clusters in different data center, cloud, and edge locations in a unified manner that enables automated policy-driven application deployment and day 2 management. AWS, Azure, and Google Cloud Platform all offer their own set of tools and technologies for DevOps, MLOps, and general operations management on their Kubernetes cloud. EMA will explore the options available to organizations aiming to maximize their ability to deploy, run, and operate applications wherever they can run in the most compliant and cost-effective manner and without changes to the application code, security policies, operations processes, and management tools.

Site Reliability Engineering: Pain Points, Trends, Requirements, and Technology Adoption Patterns

Q4 2023	This report will reveal critical success factors for implementing the SRE paradigm while exploring the importance of today's trends in DevOps, IT operations, and machine learning. Readers will learn from the successes and failures of enterprises that have transitioned to a site reliability engineering approach of optimizing cost, speed, quality, and innovation of their product and services portfolio. The study will explore how enterprises can accelerate the successful adoption of the SRE model and the critical tools and technologies in the areas of automation, root cause analytics, observability, compliance, and performance. Finally, EMA will look at how machine learning, deep learning, reinforcement learning, and similar technologies can make SREs more effective.

Network Infrastructure and Operations

Shamus McGillicuddy

AIOps-Driven Network Management

Q1 2023

In 2021, EMA research found that 90% of IT professionals believe applying AIOps technology to network management could lead to better business outcomes for an enterprise. However, IT executives were more enthusiastic about this opportunity than network engineers and architects. This year, EMA will determine whether this enthusiasm gap still exists and what vendors must do to close it.

This multi-sponsor research will draw on qualitative and quantitative research to identify how network teams are leveraging AI and ML technologies, what challenges they have with consuming the technology, and how vendors can ensure they are delivering the most value to customers.

Network Infrastructure and Operations for the Hybrid Work Enterprise

Q2 2023

The nature of work has shifted profoundly in recent years. Two years ago, 85% of network infrastructure and operations teams reported growth in the number of employees who work from home at least part-time. Only 31% of network teams considered themselves fully successful at supporting the requirements of those hybrid workers. This new multi-sponsor research project will identify how IT organizations are evolving their networks to provide secure and reliable connectivity to employees no matter where they work.

Through a combination of quantitative and qualitative research, EMA will explore the changes happening in on-premises enterprise networks. EMA will identify how network teams are updating their network observability solutions to support these hybrid workers and reveal the investments they are making for secure home office connectivity.

Establishing Trusted Network Management Tool Integration with ITSM, SIEM, and Other Systems

Q2 2023

NetOps teams often integrate their network management tools with IT systems outside the networking silo to drive operational efficiency and automation, but successful integration requires trust. For instance, many NetOps professionals tell EMA that they feel out-of-the-box integrations offered by their network management tool vendors are immature. Thus, they do custom integration, even if that custom integration doesn't deliver as much functionality as the vendor's offering.

With this market research, EMA will explore how NetOps teams establish trusted integration and how network management vendors can help them succeed. It will explore some of the most popular targets for integration, such as IT service management, security monitoring, and DevOps automation. This project will explore the role AIOps plays in driving trusted integrations. It will also identify how vendors must evolve their APIs, professional services, and customer support offerings to drive customer success with integration.

Network Infrastructure and Operations

Shamus McGillicuddy

DDI Modernization: DNS, DHCP, and IP Address Management for Multi-Cloud Enterprises

Q3 2023	IT organizations often overlook core network services, such as DNS, DHCP, and IP address management (DDI). Many enterprises attempt to use homegrown solutions, including a combination of spreadsheets and open source of free software to deliver these services. However, cloud computing, the Internet of Things, and new security requirements added a new level of complexity that requires enterprise-class DDI solutions. This multi-sponsor research will explore what drives an enterprise to adopt commercial DDI solutions, the new requirements organizations are setting for DDI, and the benefits they experience from investment in the technology. EMA will pay particular attention to hybrid cloud, automation, and security requirements.

NetSecOps: How Network Teams Build Partnerships with Cybersecurity

Q3 2023	Years of EMA research revealed that network infrastructure and operations teams are building closer partnerships with IT and cybersecurity groups, especially in support of network compliance, cloud transformation, mobility, and the Internet of Things. This new multi-sponsor research will explore best practices for how these groups collaborate on network design, implementation, and operations. EMA will explore the importance of network data as a foundation of network and security collaboration. The research will also look at how network monitoring and network automation tools can best support this collaboration.

Enterprise Network Automation: Managing Design, Deployment, and Change

Q4 2023	EMA's past research found that many IT organizations rely on a mix of homegrown and commercial tools for automating their networks. The prevalence of homegrown software suggests that many enterprises are struggling to find tools that meet all their requirements. This new multi-sponsor research project will identify where these solution gaps exist and how vendors can close them. The research will focus primarily on how IT organizations automate processes for design, deployment, and change management of networks across data centers, local-area networks, and wide-area networks. EMA will explore emerging requirements around advanced modeling, analytics, and AIOps-assisted automation.

Network Infrastructure and Operations

Shamus McGillicuddy

EMA Radar for Network Observability

Q4 2023	This report will update the 2021 "EMA Radar for Network Performance Management" using evaluation criteria that EMA updated to reflect the industry's evolution from network performance management to network observability. With this primary research, EMA will assess the core capabilities and features of leading vendors that support network fault and performance monitoring, troubleshooting, and capacity planning. The Radar will examine the overall experiences that customers have with procuring, deploying, administering, and using these products. Moreover, this report will explore how solutions address emerging observability paradigms, such as the ability to present insights and answer network managers' questions using advanced analytics and AIOps.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

API Security: The Critical Intersection Between Application Development and Security

Q4 2022	2022 will be the year in which the enterprise is forced to pay attention to application security. For years, security vendors discussed DevSecOps solutions and the benefits that they bring to the mature enterprise. Forecasted attacks on APIs and infrastructure as code (IaC) have put application security in the spotlight. 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, this research will seek to measure how far enterprises have come in protecting APIs, uncover the challenges they face in trying to secure APIs, and look at the strategies that are in place and being formulated to defend against these new types of threats.

Cyber-Threat Intelligence – Voices in the Static and Early Warning

Q4 2022	Previously available only to the largest organizations, cyber-threat intelligence (CTI) has become affordable, easy to access, and easy to use for organizations large and small. Are organizations effectively leveraging this technology? Between 2016 and 2021, the number of incidents reported to the Internet Crime Complaint Center grew from 298,728 to 847,376. This alarming exponential rate of cybercrime growth means growth of associated indicators of compromise or attack methods. More data means organizations that previously processed threat data in-house will likely be unable to do so going forward. With increasing concerns regarding zero-day vulnerabilities and the inability of vendors to keep pace with cyber-threats, organizations are turning to CTI to prevent emerging threats. This research will explore the value organizations are seeing in leveraging threat intelligence platforms and how these platforms (and their data) can be further improved.

Security Operations and Technology Megatrends: Driving Better Security Outcomes

Q4 2022	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 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.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

Security Top 3 Assessment: Endpoint/Extended Detection and Response (EDR/XDR)

Q1 2023	In this series of research analysis, EMA will assess and compare endpoint/extended detection and response vendors. The leaders will be identified and receive recognition in the review. The EDR/XDR Security Top 3 assesses feature strengths, use cases, and other capabilities of malware detection, incident response, and prevention solutions to rank how the solutions meet business needs.

Data Security as the Core of the Modern Cybersecurity Strategy

Q1 2023	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 aiming to move critical workloads and data stores to the cloud. In addition, GDPR and CCPA regulators are starting to issue violations, and as the various courts issue verdicts, the scope of how data privacy is regulated and the impacts 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. 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.

The Transformation From Cybersecurity Management to Risk Management

Q1 2023	Under various names, such as information assurance and information security, what is 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 the necessary visibility. Security must be able to communicate how proposed business tools and processes will negatively affect the business risk profile and attack surface. Security must also be able to communicate how tools they use and want to purchase will positively affect the same.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

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

Q1 2023

VPN—the core technology that enabled the recent surge in working from home—is a decades-old technology, providing a connectivity solution with very little in the way of security. Organizations are trying to better understand the value of the zero trust model while vendors shift the messaging and deliverables to take advantage of this technology. As organizations reevaluate VPNs and enterprise networking solutions, they are turning to zero trust solutions as the connectivity and end-user security solutions of the future. 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. EMA will also evaluate the requirements that organizations have when implementing a zero trust project.

DevSecOps and Securing Today's Enterprise

Q2 2023

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 risks of vulnerabilities, such as the recent Log4j? Is commercial software more secure, or still susceptible to problems, 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.

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

Q2 2023

Since 1971, email has increasingly become part of daily life for most businesses across the globe. There have been great improvements across the IT industry in securing email to protect confidentiality and verifiability of this critical business communication tool. 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 in 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 info (PII) a serious security risk to organizations. How are organizations addressing this major security concern without impeding productivity? This research will examine today's email security methods and tools and examine where the industry is struggling—and where they are succeeding.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

Are Security Best Practices Enough to be Quantum-Ready?

Q2 2023

The security space has been abuzz with news about quantum computing, and it is not a matter of *if* it is coming, but *when* it is coming. The US government is already evaluating quantum encryption standards and has 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 for most organizations that is "good enough?" Are there strategies and tools that the enterprise should adopt to be quantum-ready? Since many workloads and data stores have migrated (or are being migrated) to the cloud, is this a problem for the cloud service providers (CSPs) to deal with? 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 quantum computing, and how their organizations plan to invest to get ready for the eventual surge in quantum computing to protect their data.

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

Q2 2023

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 antivirus vendors processing over 450,000 new samples each day. With this huge increase in malware, antivirus vendors struggle to keep up—not only with signatures for new variants, but even 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 are organizations being impacted by today's malware? 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 combating it, and where these efforts are succeeding or failing.

Investing in Your Most Valuable Asset – Cybersecurity Workforce Development

Q2 2023

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. 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? Are organizations more secure? This research will examine organizations' investments in strengthening their cybersecurity workforce and observed return on this investment.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

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

Q3 2023	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?

Q3 2023	Organizations have to 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 the ability to achieve outcomes. Whether they 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.

NDR and XDR – Bridging the Gap Between the NOC and the SOC

Q3 2023	For many mature organizations, the Network Operations Center (NOC) was the heartbeat of everything technical in the enterprise. The NOC served as the eyes and ears of business and technical leadership and was usually the best indicator of issues in the organization. In recent years, the Security Operations Center (SOC) has become the priority, often merging with the NOC or replacing the NOC outright. Business and technology leaders have pivoted spending and priorities to internal and external cyber-attacks, deploying tools and resources to deal with emerging risks and threats. Security services and tools vendors have acknowledged this shift and have changed their messaging to cater to security influencers in the organization. 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 spending on network operations tools and services compared to security tools and services. The research will also look at the prioritization of security over network spending in technology departments within the enterprise.

Security, Risk, and Compliance Management

Chris Steffen and Ken Buckler

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

Q4 2023	Data privacy regulations are becoming more relevant to every size of business. GDPR and CCPA 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 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 tolls 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 enterprise. 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 address 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 and the needs that those organizations have when dealing with their data estates.

Security Compliance Frameworks – Are They Enough?

Q4 2023	PCI, DISA STIG, FISMA, NIST, and CIS all provide compliance frameworks to secure enterprises—but 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 if they are enough to secure organizations, or if additional steps need to be taken to be truly secure.

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

Q4 2023	As the cybersecurity industry continues to struggle with a workforce shortage, with almost three 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 influence service-level agreements and cost? 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.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data 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 EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

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

4218.031323