

2026

Enterprise Management Associates (EMA)
Research Calendar

Information Security, Risk and Compliance Management

Information Security, Risk and Compliance Management

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

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

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

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

Information Security, Risk and Compliance Management

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

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

Supply Chain Security: Enterprise Strategies for Mitigating Cybersecurity Risk

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

Data Security and Privacy at the Endpoint in a Distributed World

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

Information Security, Risk and Compliance Management

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

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

Are Security Best Practices Enough to be Quantum-Ready?

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

Identity Attacks in Cyber: Are Current Defenses Keeping Up?

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

Information Security, Risk and Compliance Management

Deepfakes and the New Dawn of Social Engineering

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

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

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

Behavioral Analytics and AI for Proactive Threat Hunting Across Diverse Endpoints

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

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

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

Information Security, Risk and Compliance Management

Securing Edge Computing: Balancing Performance and Protection in Distributed Systems

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

Cyber Threat Intelligence and Proactive Defense

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

EMA™ PRISM Reports

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

EMA™ PRISM Report for Cloud Native Security & Container Security

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

Information Security, Risk and Compliance Management

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

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

EMA™ PRISM Report for Data Loss Prevention (DLP)

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

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

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

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

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

Information Security, Risk and Compliance Management

EMA™ PRISM Report for SASE

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

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

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

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

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

EMA™ PRISM Report for Email Security

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

Information Security, Risk and Compliance Management

EMA™ PRISM Report for Attack Surface Management (ASM)

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

EMA™ PRISM Report for SIEM

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

EMA™ PRISM Report for Deception Technology

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

EMA™ PRISM Report for Threat Hunting

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

Information Security, Risk and Compliance Management

EMA™ Radar Report for Privileged Access Management (PAM)

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

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

Information Security, Risk and Compliance Management

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

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

Ken 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).



Chris Steffen
VP of Research

Certifications

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



Ken Buckler
Research Director

Certifications

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

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.

©2025 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.