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

EMA™ PRISM Report for API Security

Summary Report Spotlighting Cequence

August 2025

By **Christopher M. Steffen, CISSP, CISA, CCZT;** VP of Research
Information Security, Risk, and Compliance Management
Enterprise Management Associates (EMA)

Table of Contents

Executive Summary

Welcome to the Enterprise Management Associates™ (EMA) PRISM report on API security solutions. EMA is an industry-leading analyst firm specializing in a wide range of technology areas, including cybersecurity. We are dedicated to providing comprehensive research, analysis, and insights to help organizations make informed decisions about their technology investments.

The EMA PRISM report is a broad overview of a particular product set in a larger technology space. It is designed to provide practitioners and business leaders with a starting point for solutions in a common vertical. It uses publicly available information and sentiments, as well as the expertise of EMA researchers, to create an easy to understand and digestible overview of significant vendors/solutions in a space. It is NOT meant to be a detailed or thorough examination of the solutions in that vertical, nor does it include all of the solutions in that vertical.

The information presented in this report acts as a starting point for decision-makers and practitioners to evaluate the vendors and solutions that best align with your organization's needs and requirements.

Understanding API Security

API security is the practice of protecting application programming interfaces (API) from threats. This includes measures to prevent attacks, misuse, and data breaches by implementing controls to secure the communication, data, and logic exposed through APIs. At its core, it's about ensuring that only legitimate users and applications can access and interact with an API, and that the data exchanged remains confidential and intact.

As businesses increasingly rely on APIs to connect applications, share data, and power digital services, API security has become a non-negotiable part of a comprehensive cybersecurity strategy. APIs are a primary attack vector, representing a direct gateway to an organization's critical data and services. A single vulnerability can lead to massive data breaches, service disruptions, financial losses, and reputational damage. Effective API security mitigates these risks, protecting sensitive information like customer data and intellectual property, ensuring business continuity, and helping companies comply with regulations like GDPR and CCPA.

The landscape of API security is rapidly evolving, driven by the sophistication of modern threats. A key trend is the shift from traditional perimeter-based security to a more granular, API-centric approach. Modern solutions are moving beyond basic API gateways and WAFs to offer specialized capabilities. This includes continuous API discovery and inventory to identify and secure all APIs, including shadow APIs and zombie APIs. Another major trend is the use of AI and machine learning to analyze API traffic for behavioral anomalies, enabling the detection of sophisticated bot attacks and business logic abuse in real time. Finally, there's a growing emphasis on shift-left security, integrating security testing and scanning earlier in the API development lifecycle to fix vulnerabilities before they are deployed.

Solutions the EMA PRISM Report Evaluates

This EMA PRISM report evaluates the following API security solutions:

42Crunch API Security Platform

Akamai API Security

Akto

APIsec (API Security Testing Tool)

Axway Amplify Platform

Barracuda Networks API Protection (part of Application Protection)

Beagle Security Automated API Security Testing

Cequence Security Unified API Protection (UAP) Platform

Cloudflare API Shield

Data Theorem API Secure

F5 Networks F5 Distributed Cloud Services/API Security

IBM API Connect

Imperva Unified API Security Platform

Kong API Gateway

Palo Alto Networks Prisma Cloud

Postman Pynt (Postman API Network)

Rapid7 InsightAppSec

Salt Security API Protection Platform

Sophos Web Application Firewall

StackHawk Dynamic Application Security Testing

Traceable AI Platform

Wallarm API Security Platform

The EMA PRISM Report

The security solutions landscape is constantly evolving, and organizations face a daunting challenge: selecting the optimal security solutions to safeguard their digital assets. With a myriad of vendors and products vying for attention, it can be difficult to discern the truly significant offerings. The Enterprise Management Associates (EMA) PRISM report is a novel approach designed to illuminate the path, providing a comprehensive and objective evaluation of security solutions.

PRISM, an acronym for **PR**oduct and Functionality, **I**ntegrations and Operability, and **S**trength and **M**aturity, offers a structured framework for assessing security vendors and their offerings. By examining these key dimensions, the PRISM report provides a nuanced understanding of a solution's capabilities, limitations, and potential impact on an organization's security posture.

The **Product and Functionality** section evaluates the core capabilities of a security solution. It assesses the solution's ability to deliver on reported features compared with other solutions and identifies solutions that offer robust protection against a wide range of cyber threats.

The **Integrations and Operability** section explores the solution's compatibility with existing security infrastructure and its ease of use. It evaluates the solution's ability to integrate seamlessly with other security tools, its user-friendliness, and its ability to provide meaningful analytics and reporting while identifying solutions that can enhance an organization's overall security posture without adding unnecessary complexity.

The **Strength and Maturity** section examines the vendor's financial stability, market reputation, and product innovation. It also assesses the solution's total cost of ownership, time to value, and its long-term vision and roadmap, highlighting vendors that are committed to delivering innovative and effective security solutions.

The EMA PRISM report is a powerful tool for organizations seeking to make informed decisions about their IT and security investments. The report empowers organizations to select the best solutions and tools to protect their critical assets and mitigate risk.

EMA PRISM Evaluation Overview

The EMA PRISM report combines public user sentiment and analyst analysis with vendor feedback to develop a quick-glance profile of a vendor and its product strengths in a segment of the industry.

The PRISM report scoring methodology is crafted to address various aspects of vendor offerings, found in Product and Functionality, Integrations and Operability, and Strength and Maturity. EMA understands that every organization has unique needs and hopes that the information gathered for this report will enable organizations to tailor their vendor selection to best align with their specific requirements.

Evaluated Categories

Product and Functionality

- Comprehensive API Discovery and Inventory
- Real-Time Behavioral Analysis
- Automated Threat Detection
- Full API Lifecycle Coverage (Shift-Left & Shield-Right)
- Robust Authentication and Authorization Enforcement
- Vulnerability Management and Testing
- Data Security and Privacy Protection
- Rate Limiting and Bot Management

Integrations and Operability

- Analytics & Reporting
- Integrations and Compatibility
- Ease of Use & Management
- End-User Support

Strength and Maturity

- Vendor Strength
- Time to Value
- Total Cost of Ownership
- Strategy and Vision

Product and Functionality

Comprehensive API Discovery and Inventory

This section evaluates how well a solution automatically finds and catalogs all APIs, including undocumented "shadow" APIs. It assesses the depth of the inventory, including endpoint details and data types, to provide a complete view of the API attack surface. A strong inventory is the foundation for effective API security, since you cannot protect what you don't know exists.

Real-Time Behavioral Analysis

This section evaluates the use of AI/ML to establish normal API behavior and detect anomalies in real time. It measures a solution's ability to identify sophisticated, non-signature-based attacks, like business logic abuse and insider threats, by analyzing traffic patterns and user behavior for subtle deviations from the norm.

Automated Threat Detection

This section evaluates a solution's ability to automatically identify and alert on malicious activity. It includes detection of known threats, like the OWASP API Security Top 10, as well as novel attacks. The focus is on the speed and accuracy of a system's ability to recognize and respond to threats without human intervention.

Full API Lifecycle Coverage (Shift-Left & Shield-Right)

This section evaluates a solution's ability to provide security across the entire API lifecycle. Shift-left refers to security testing during development, while shield-right covers runtime protection in production. A strong solution provides continuous security from code creation to live deployment, preventing and mitigating vulnerabilities at every stage.

Robust Authentication and Authorization Enforcement

This section evaluates how effectively a solution enforces access controls. It assesses the mechanisms used to verify user and application identities (authentication) and the actions they are permitted to perform (authorization). Strong enforcement is critical for preventing unauthorized access and ensuring the principle of least privilege.

Vulnerability Management and Testing

This section evaluates the tools and processes for proactively identifying and managing security weaknesses in APIs. It includes continuous scanning, penetration testing, and security testing integrated into the development pipeline. The goal is to find and remediate vulnerabilities before malicious actors can exploit them in a production environment.

Data Security and Privacy Protection

This section evaluates a solution's ability to protect sensitive data transmitted through APIs. It focuses on features like encryption, data loss prevention (DLP), and granular access controls to prevent data exposure. The goal is to ensure confidential information, such as PII, remains private and secure in compliance with regulations.

Rate Limiting and Bot Management

This section evaluates a solution's effectiveness in controlling API traffic to prevent abuse and ensure availability. It assesses features that restrict the number of requests from a single source (rate limiting) and differentiate between legitimate human or bot traffic and malicious automated attacks, like brute force or content scraping.

Integrations and Operability

Analytics & Reporting

This section evaluates the quality and comprehensiveness of the solution's analytics and reporting capabilities. This includes the ability to generate meaningful insights, customize dashboards, and integrate with other security tools.

Ease of Use & Management

This section evaluates the user-friendliness and efficiency of the solution's management interface. This includes the ease of configuration, the automation of tasks, and the overall user experience.

Integrations and Compatibility

This section evaluates the solution's ability to integrate with other security tools and platforms. This includes the availability of APIs, the compatibility with different technologies, and the ease of integration.

End-User Support

This section evaluates the quality of the vendor's customer support. This includes response time, technical expertise, and the availability of training and documentation.

Strength and Maturity

Vendor Strength

This section evaluates the vendor's financial stability, market reputation, and commitment to security. This includes the vendor's track record, customer satisfaction, and product innovation.

Total Cost of Ownership

This section evaluates the overall cost of acquiring, deploying, and maintaining the solution. This includes licensing costs, hardware requirements, and operational overhead.

Time to Value

This section evaluates the speed at which the solution can be deployed and deliver value. This includes the ease of deployment, the time to initial protection, and the return on investment.

Product Strategy and Vision

This section evaluates the vendor's long-term vision for the product and its alignment with industry trends. This includes the product roadmap, future development plans, and the commitment to addressing emerging threats.

Evaluation Methodology

All vendors are evaluated based on publicly available data. Publicly reviewed data includes, but is not limited to:

- Vendor documentation and public knowledgebase
- Media and news articles
- Social media posts by users of the product/solution
- Questions and answers on public help forums, including vendor help forums and third-party help forums, such as StackExchange

In addition to evaluation based on publicly available data, EMA offers all selected vendors the chance to provide feedback regarding their solution profile before final publication.

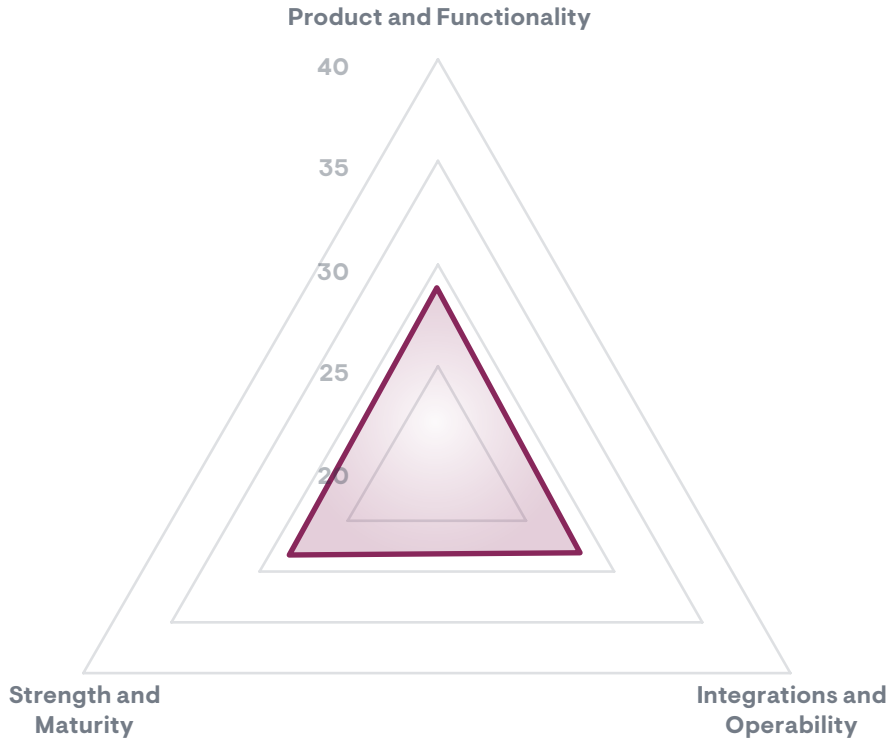
EMA evaluates all responses and scoring based on information within the last several years, utilizing the most up-to-date information possible. EMA evaluates each data point on a weighted scale, with some criteria weighing more heavily on final scoring.

Solution Evaluation

The EMA PRISM report showcases each vendor solution with a profile that highlights the evaluated categories of the solution, displayed on a spectrum chart. All points are rated on a weighted scale, with fractional points allowed. The overall vendor score is determined by taking the sum of all data points. An overview of the product and our findings will be included, as well as several bullet points highlighting the product's key differentiators.

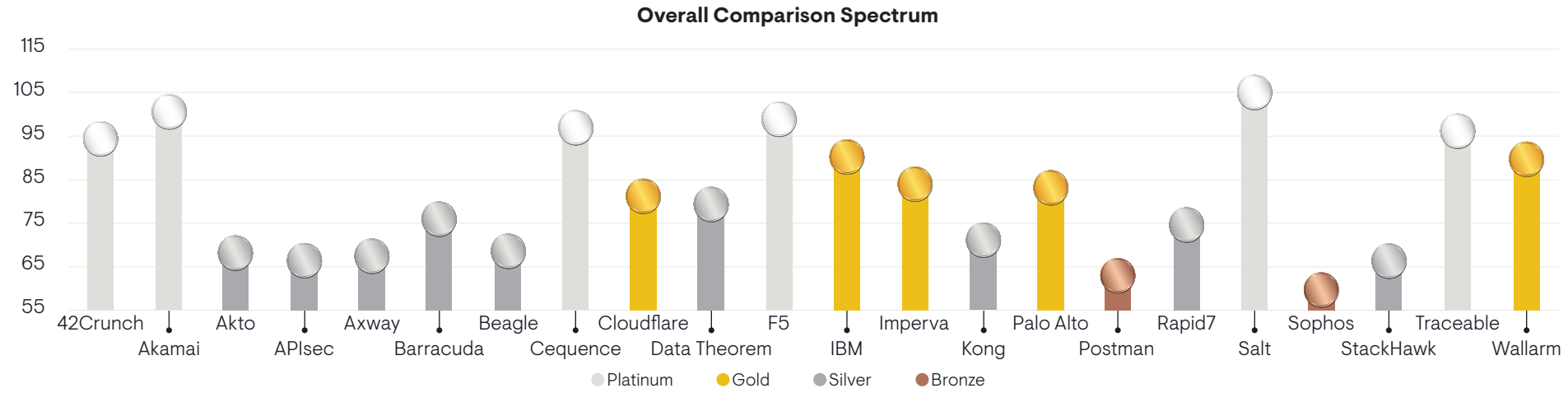
For the EMA PRISM report, each compared solution includes their overall spectrum score, as well as a category comparison spectrum.

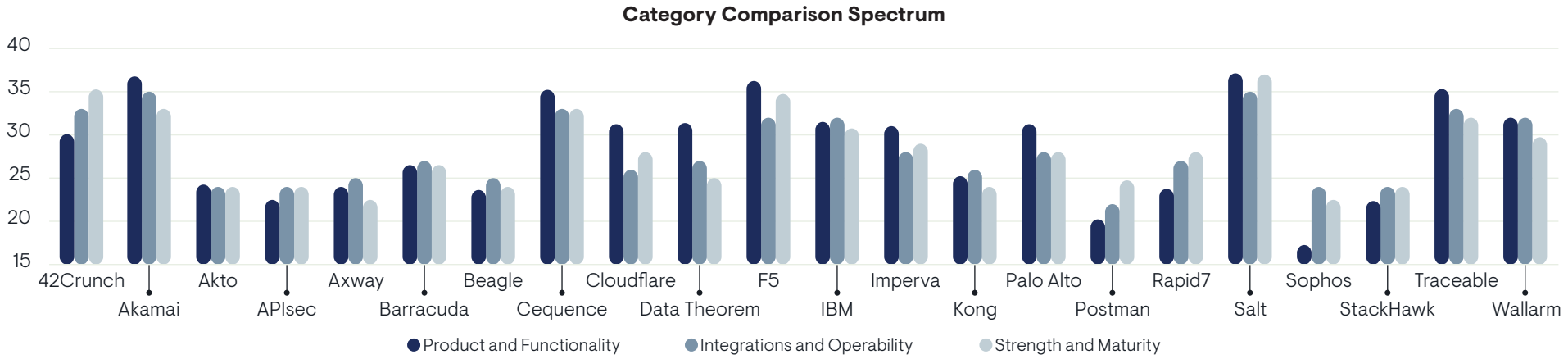
Product and Functionality	Platinum	40.00
Integrations and Operability	Platinum	40.00
Strength and Maturity	Platinum	40.00
Overall	**Platinum**	**120.00**



On the EMA PRISM Report

The EMA PRISM report defines the overall value of any solution as a spectrum of three characteristics: Product and Functionality, Integrations and Operability, and Strength and Maturity.





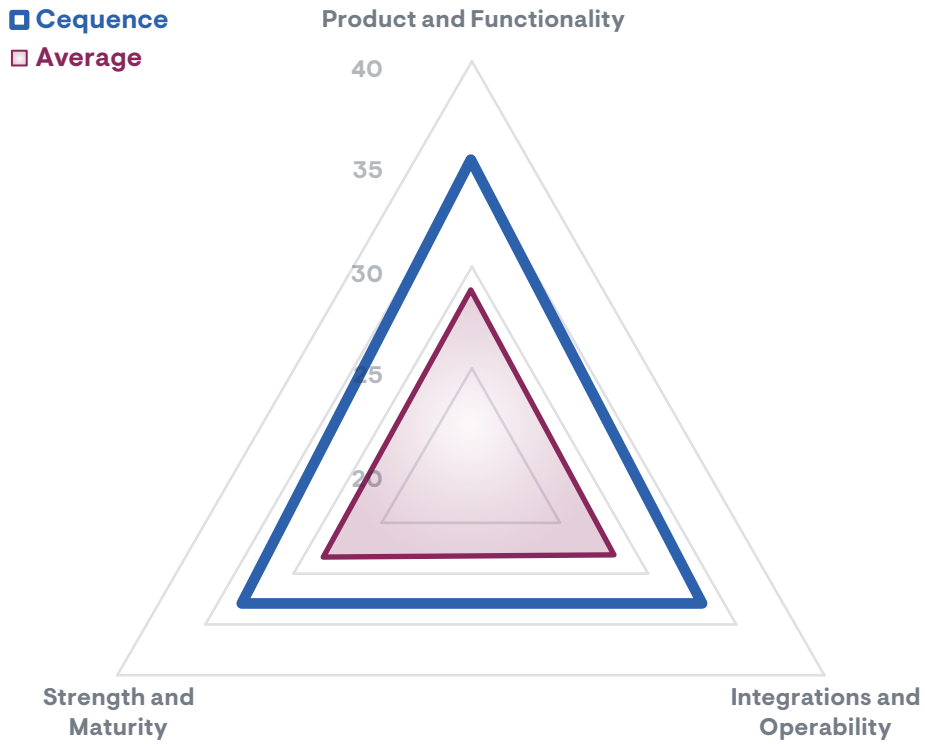
CEQUENCE

Solution: **Cequence Unified API Protection (UAP) Platform**

Website: **https://www.cequence.ai/unified-api-protection/**

The Cequence Unified API Protection (UAP) Platform provides a comprehensive security solution designed to protect modern cloud native applications from API-related threats. It encompasses a wide array of security features that not only shield APIs against malicious activities, but also offer insights that enhance operational efficiency for developers and security teams alike.

Product and Functionality	Platinum
Integrations and Operability	Platinum
Strength and Maturity	Platinum
Overall Ranking	**Platinum**



Key Capabilities

- Comprehensive API Discovery and Inventory: Cequence automatically discovers internal, external, and third-party APIs as well as edge, infrastructure, gateway, and hosting providers and inventories all APIs within an organization, ensuring that all endpoints are accounted for and evaluated for vulnerabilities.
- Automated Threat Detection: The platform utilizes advanced algorithms to detect unusual patterns and potential threats in real time, natively mitigating to bring Mean Time to Respond (MTTR) to API attacks to near-zero.
- Robust Authentication and Authorization Enforcement: It integrates seamlessly with various identity providers to ensure that authentication and access policies are consistently enforced across APIs.

Key Differentiators

- Full API Lifecycle Coverage (Shift-Left & Shield-Right): Cequence offers a proactive approach to API security by integrating security measures early in the development process (shift-left) while continuously protecting live APIs (shield-right).
- Real-Time Behavioral Analysis: Unlike many traditional security solutions, Cequence leverages machine learning to perform real-time behavioral analysis, allowing for more precise threat detection and mitigation.
- Prevent Sensitive Data Exposure: Cequence automatically identifies and masks sensitive data using ML-based rules with predefined and customizable data patterns. Sensitive data is identified wherever it is, without having to explicitly define in advance the specific APIs that transact it or what data is sensitive.
- Vulnerability Management and Testing: The platform not only identifies vulnerabilities, but also provides actionable testing capabilities to help organizations remediate these issues quickly. Test plans can be automatically generated from Postman collections or API specifications (which, if missing can be created by the system, removing a heavy manual burden).

Product and Functionality

Cequence's Unified API Protection platform is recognized for its strength and maturity in the API security landscape. With its extensive feature set that integrates discovery, analysis, and protection, Cequence stands out as a vital solution for organizations seeking to secure their API ecosystems. The emphasis on real-time threat detection and machine learning capabilities positions Cequence as a leader specialized in proactive security management. This maturity reflects a commitment to delivering consistent quality, highlighting its ability to adapt to the diverse and evolving threat landscape in API security.

Integrations and Operability

The Cequence UAP Platform excels in integrations and operability by seamlessly aligning with existing development and security workflows within organizations. Comprehensive compatibility with CI/CD pipelines, DevOps tools, and enterprise systems ensures that security measures are embedded early and consistently throughout the API lifecycle. The platform's user-friendly management interface and detailed analytics tools further enhance its operability, providing teams with the insights needed to fine-tune their API security strategies. Additionally, with strong vendor support, organizations experience a smooth onboarding process and continual guidance, facilitating an efficient transition toward a robust API protection regime.

Strength and Maturity

Cequence Security demonstrates considerable strength and maturity through its effective vendor strategy and visionary leadership in the domain of API protection. By focusing on streamlining API security with a comprehensive, all-in-one solution, Cequence reduces the total cost of ownership while ensuring rapid deployment and time to value for customers. The vendor's robust customer support and engagement further solidify its reputation, since customers benefit from expert guidance and resources that empower them to maximize the platform's capabilities. Together, these elements reflect Cequence's commitment to fostering secure, resilient API ecosystems for organizations of all sizes.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

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