EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

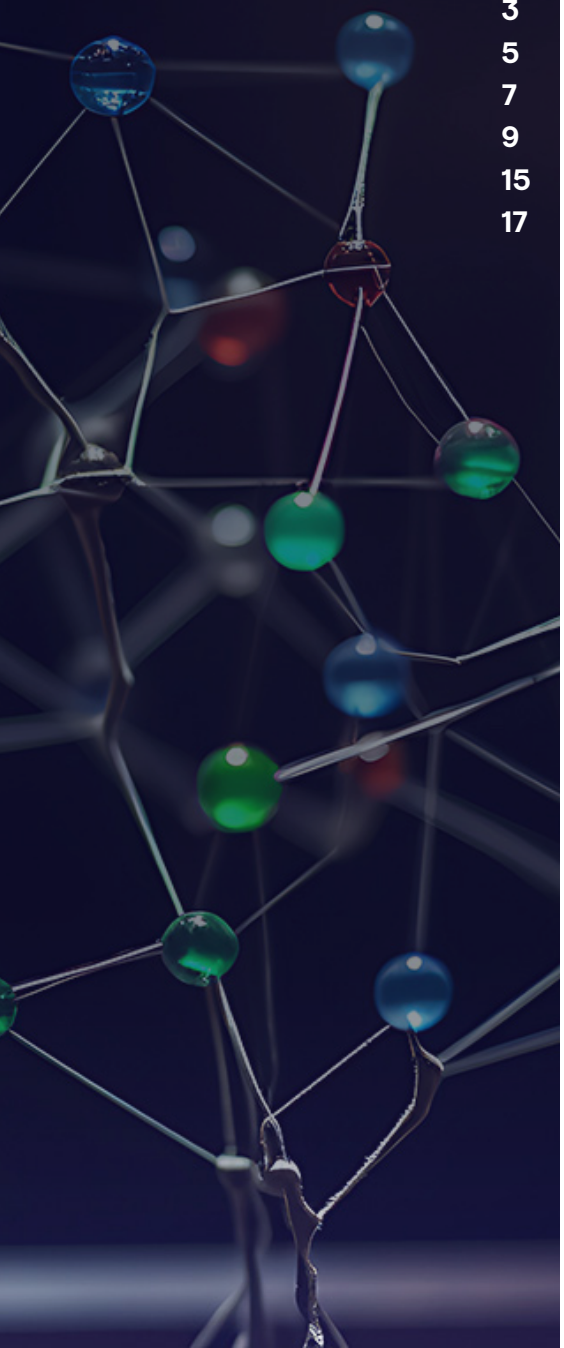
Prepared for:
ZERO Networks

No Longer a Networking Science Project:
The Maturing Microsegmentation Market

June 2025 EMA Research Report
By **Christopher M. Steffen, CISSP, CISA**, VP of Research and **Ken Buckler, CASP**, Research Director
Information Security, Risk and Compliance Management



Table of Contents



1 Introduction
3 Understanding Microsegmentation
5 Key Findings
7 Voices of the Survey – Respondent Quotes
9 Microsegmentation Trends
15 EMA Perspective
17 Research Methodologies and Demographics



Introduction

Microsegmentation, once considered a complex and niche security solution, is rapidly maturing into a mainstream enterprise defense strategy. The escalating sophistication of cyber threats and the increasing recognition of the benefits microsegmentation offers in terms of reduced attack surface, enhanced breach containment, lateral movement prevention, and improved overall security posture drove this evolution.

However, the path to widespread adoption is not without its challenges. Complex IT environments, skill shortages, and the need for significant upfront investments hinder the rapid uptake of microsegmentation. Vendors often face hurdles in educating the market about the technology's value proposition and differentiating their offerings in a crowded marketplace. For some vendors, getting the market to understand that they can achieve microsegmented networks quickly, but also with low friction, is a challenge – the idea that adoption of a new network technology doesn't have to be traumatic to the IT teams and the end users is something that most enterprises have never experienced, and have difficulty believing is possible.

For this research project, Enterprise Management Associates (EMA) surveyed 145 IT professionals, information security practitioners, and technology business leaders across all verticals to revisit and discover their attitudes and perspectives around microsegmentation solutions. The research also evaluated the capabilities of the solutions they are considering, as well as the barriers to adoption of microsegmentation solutions.



Understanding Microsegmentation

Microsegmentation is a network security technique that divides data center and cloud networks into small, isolated segments, down to individual workloads. This granular isolation enhances security by limiting lateral movement within a network, drastically reducing the attack surface. Unlike traditional perimeter-based security, which focuses on keeping threats out, microsegmentation assumes breaches can and will occur, and aims to contain them swiftly within a defined segment, preventing widespread damage.

The importance of microsegmentation stems from its ability to implement a zero trust security model, in which no user, device, or application is inherently trusted, regardless of its location. This is crucial for protecting sensitive data, intellectual property, and critical applications from advanced persistent threats, ransomware, and insider threats. By isolating workloads, organizations can enforce least-privilege access, significantly improving compliance with regulations like GDPR and HIPAA.

Current trends in microsegmentation include its increasing adoption in hybrid and multi-cloud environments, driven by the need for consistent security policies across diverse infrastructures. The rise of agentless microsegmentation solutions simplifies deployment and management, while AI and machine learning are being leveraged for automated policy creation, anomaly detection, and predictive threat mitigation. Furthermore, integration with identity-based security and network orchestration platforms is evolving to provide more dynamic and context-aware segmentation, making it an indispensable component of modern cybersecurity strategies.



Key Findings

- **33.1%** The ability to instantly quarantine and contain threats is perceived as the greatest benefit of microsegmentation.
- **65.5%** A significant majority of respondents considers microsegmentation to be extremely important for cyber defense.
- **40.7%** A plurality believes automated policy creation and lifecycle management will be an extremely important differentiator.
- **47.6%** Nearly half consider fast, automated asset discovery and tagging extremely important for future differentiation.
- **50.3%** A majority views integration with multi-factor authentication as extremely important for future differentiation.
- **42.8%** Real-time threat intelligence to dynamically update microsegmentation policies received the most mentions for effective defense against lateral movement and ransomware.
- **95.8%** The number of respondents who consider microsegmentation to be extremely important or very important for cyber defense.



Voices of the Survey – Respondent Quotes

Select Open-Ended Responses

Describe your perspectives on microsegmentation, including any information about how your organization is utilizing, evaluating, or implementing microsegmentation in your environments.



Microsegmentation is an approach that isolates workloads and applications by creating small, distinct segments, enabling granular security controls and reducing the potential attack surface.



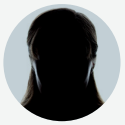
Microsegmentation is absolutely essential in a hospital health care environment such as ours. This allows our information technology department to deploy target solutions to control data flow, limit unauthorized access, and rapidly detect threats within the network.



Microsegmentation enhances security. It creates granular network controls. We're actively evaluating its implementation to isolate critical assets and limit lateral threat movement within our cloud environments.



Microsegmentation is a game-changer for security, especially in a world in which threats move fast. Traditional firewalls are not enough, because attackers can easily get in and disrupt it.



Microsegmentation is essentially about breaking down a network into smaller, isolated zones. Instead of one big network, you have lots of tiny ones. This way, if a hacker gets in, they can't move around easily and access everything.



Microsegmentation represents a proactive approach to cybersecurity by isolating workloads and applying tailored security measures at a granular level. Its implementation requires careful planning and ongoing evaluation, but offers significant benefits in terms of risk reduction and improved incident response capabilities. We utilize this to isolate incidents to minimize their impact on the business.



Zero trust has become profoundly important to our industry, and we were early adopters of microsegmentation to maximize its potential. Due to our compliance and privacy demands, we needed to minimize our attack surface as much as possible. This allows us unprecedented visibility over our networks at the minor cost of slightly diminished velocity.



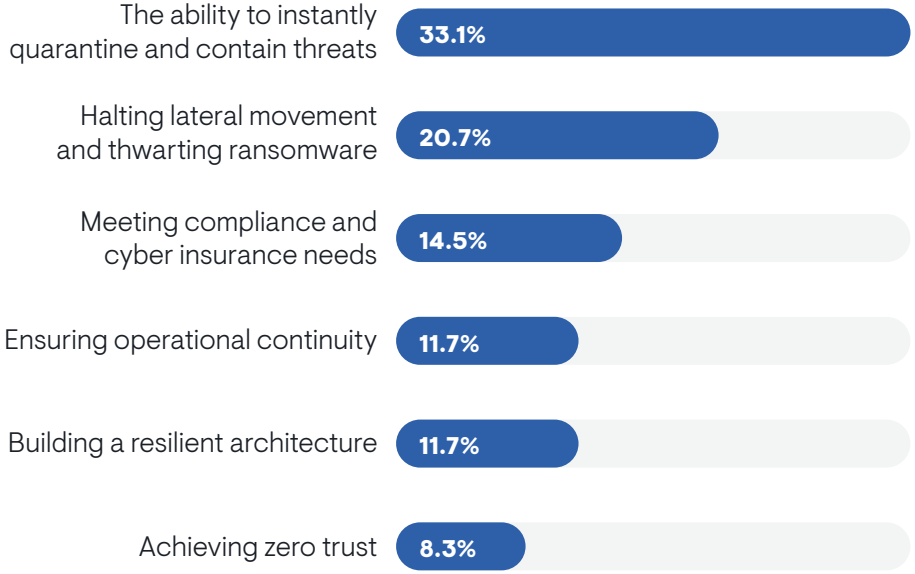
Microsegmentation Trends

The most significant perceived benefit of network microsegmentation is the ability to instantly quarantine and contain threats, cited by 33.1% of respondents. This highlights the value users place on rapid response and limiting the blast radius of security incidents.

Closely following at 20.7% is the benefit of halting lateral movement and thwarting ransomware. The emphasis on immediate containment suggests a priority in minimizing active damage. Other benefits include meeting compliance and cyber insurance needs (14.5%), ensuring operational continuity and building a resilient architecture (both at 11.7%).

The data indicates that the primary driver for adopting microsegmentation is its capability to quickly isolate and neutralize security threats, underscoring its importance in active incident response and damage control.

What do you perceive to be the greatest benefit of using microsegmentation?

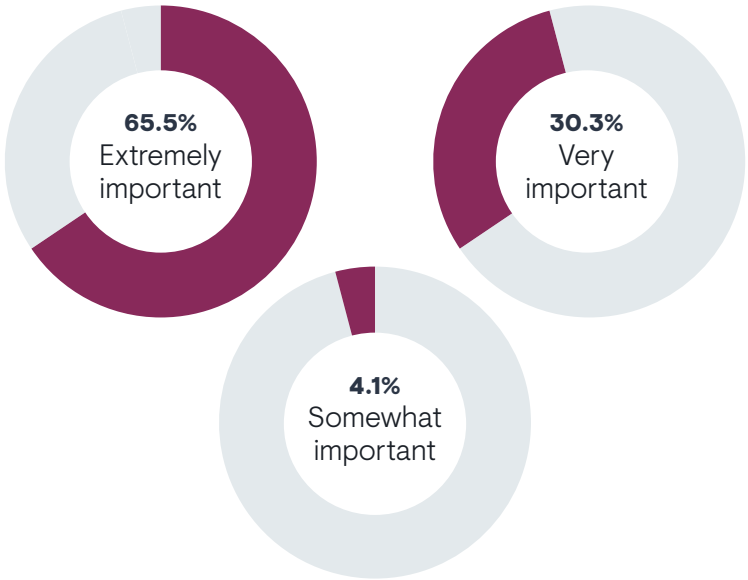


The majority of respondents consider microsegmentation for cyber defense extremely important, while an additional 30.3% view it as very important. This means that nearly 96% of respondents recognize the substantial value of microsegmentation in enhancing network security.

Using microsegmentation for granular controls is clearly perceived as essential in today's threat landscape, and microsegmentation is viewed as an important method of containing potential breaches and reducing the attack surface.

Only a small fraction (4.1%) believe microsegmentation is merely somewhat important, indicating a strong consensus on its necessity. This data underscores the growing recognition of microsegmentation as a fundamental component of a robust cyber defense strategy, but also highlights the need for further education on the benefits of microsegmentation.

How important do you consider microsegmentation to be for cyber defense?



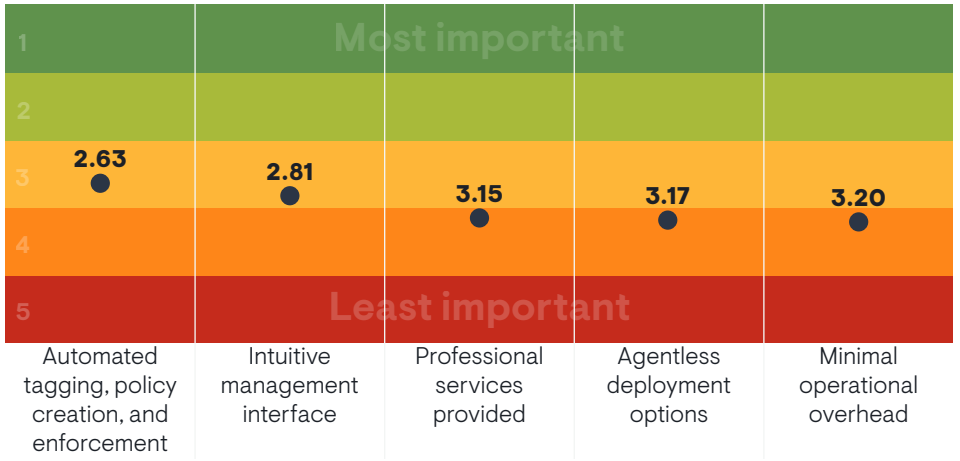
From the perspectives of ease of deployment and ongoing management, the data shows that automated tagging, policy creation, and enforcement are considered the most important requirements when selecting a modern microsegmentation solution, with an average rating of 2.63 (with a rating of one being the most important of the listed choices). This indicates that users prioritize features that streamline the initial setup and ongoing administration of microsegmentation policies.

Following closely is an intuitive management interface at 2.81, highlighting the importance of user-friendliness for efficient operations. The need for professional services provided (3.15), agentless deployment options (3.17), and minimal operational overhead (3.20) are also important, but appear to be slightly lower priorities compared to automation and ease of use.

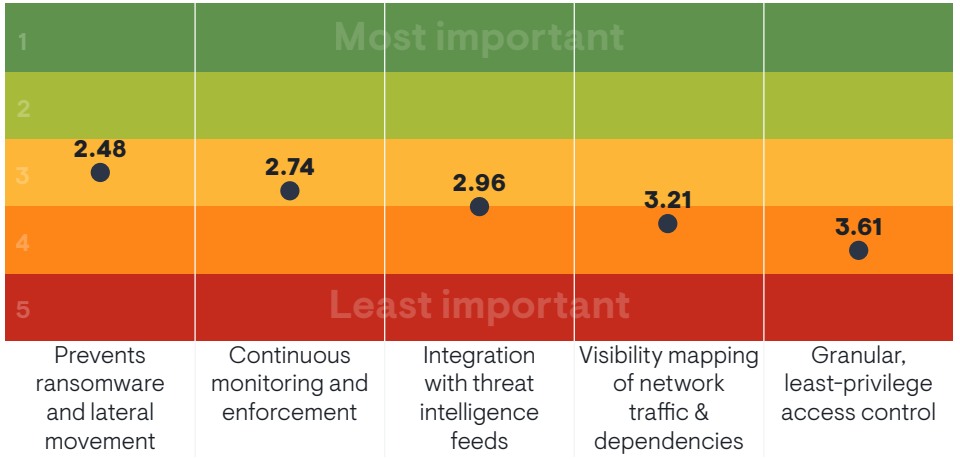
When considering security and threat protection, preventing ransomware and lateral movement emerges as the most critical requirement, with an average rating of 2.48. This aligns with the earlier data point that emphasizes the importance of containing threats.

Continuous monitoring and enforcement (2.74) and integration with threat intelligence feeds (2.96) are also highly valued for maintaining a strong security posture. Visibility mapping of network traffic and dependencies (3.21) is seen as important for understanding the environment, while granular, least-privilege access control (3.61), although a core principle of microsegmentation, appears to be relatively less emphasized in this specific ranking.

From ease of deployment and solutions management perspectives, what requirement is most important to you when selecting a modern microsegmentation solution?



From security and threat protection perspectives, what requirement is most important to you when selecting a modern microsegmentation solution?



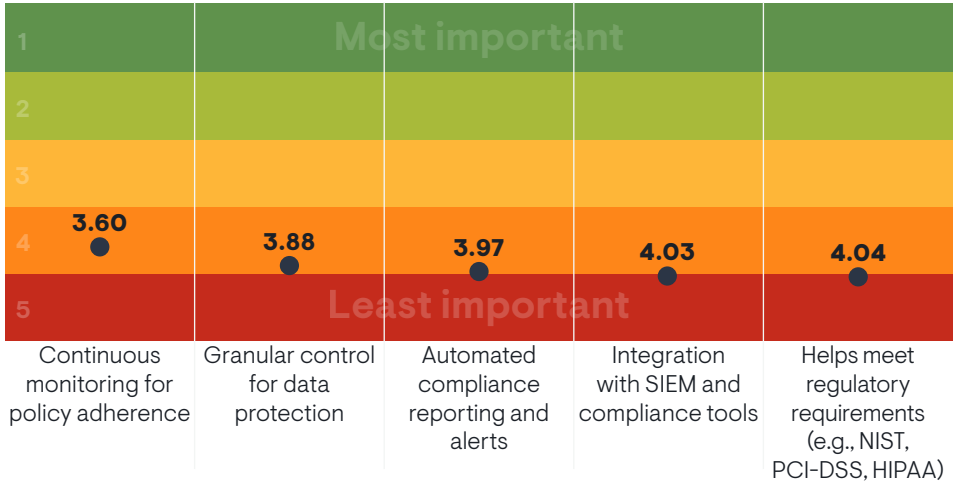
From a compliance and visibility standpoint, the most important requirement when selecting a microsegmentation solution is continuous monitoring for policy adherence, with an average rating of 3.60. This suggests that ensuring ongoing compliance with defined segmentation policies is a key concern.

Closely following is granular control for data protection at 3.88, highlighting the need to protect sensitive information through precise segmentation. Automated compliance reporting and alerts (3.97), integration with SIEM and compliance tools (4.03), and the ability to help meet regulatory requirements (4.04) are also considered important, but appear to be slightly lower priorities compared to continuous monitoring and granular data protection.

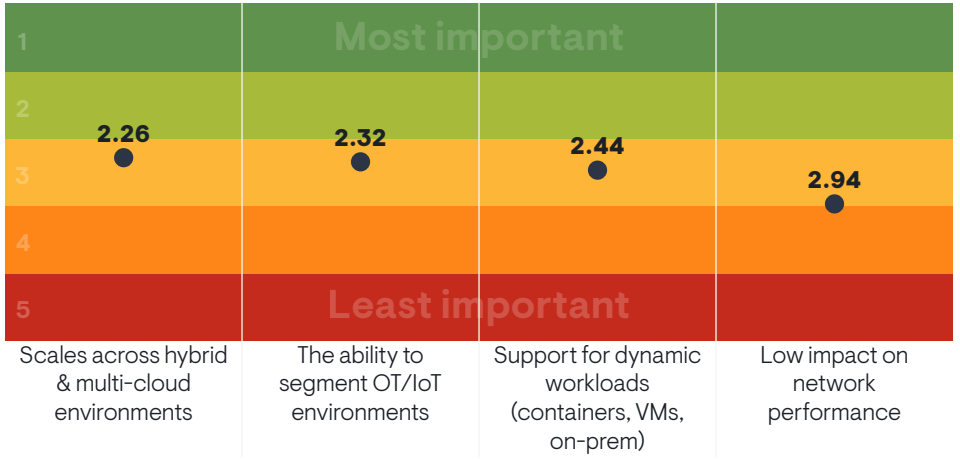
Regarding performance and scalability, the ability to scale across hybrid and multi-cloud environments is deemed the most important requirement, with an average rating of 2.26. This underscores the need for microsegmentation solutions that can seamlessly adapt to diverse and evolving infrastructure.

The ability to segment OT/IoT environments (2.32) and support for dynamic workloads (2.44) are also highly valued, reflecting the growing complexity of modern IT environments. Maintaining a low impact on network performance (2.94) is also an important consideration to ensure that security measures don't hinder operational efficiency.

From a compliance and visibility perspective, what requirement is most important to you when selecting a modern microsegmentation solution?



From a performance and scalability perspective, what requirement is most important to you when selecting a modern microsegmentation solution?

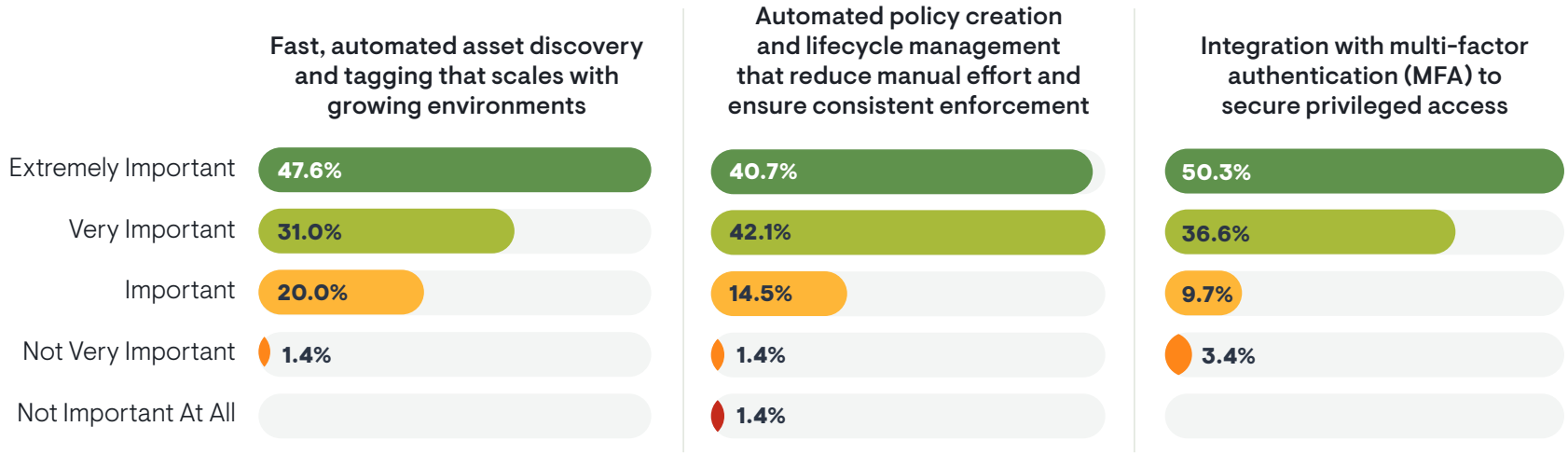


Looking 1-2 years ahead, a significant majority of respondents (40.7% extremely important, 42.1% very important) believe that automated policy creation and lifecycle management will be a key differentiator for leading microsegmentation solutions. Only a small fraction (2.8%) consider this capability to be not very or not at all important, reinforcing the widespread recognition of the need for enhanced automation in managing microsegmentation at scale.

Fast, automated asset discovery and tagging that scales with growing environments is perceived as a crucial differentiator for future microsegmentation solutions. Nearly half of the respondents (47.6%) consider this capability extremely important, with another 31% rating it as very important. The ability to automate this foundational process is seen as essential for effective and scalable microsegmentation deployments, with only a small minority (1.4%) deeming it not very important.

A majority consider that integration with multi-factor authentication to secure privileged access will be a significant differentiator for leading microsegmentation solutions in the coming 1-2 years, rating it extremely important (50.3%), and an additional 36.6% view it as very important. By integrating with MFA, these solutions can provide an additional layer of security, preventing unauthorized modifications and bolstering the overall integrity of the microsegmented environment.

Looking ahead 1-2 years, how significantly do you believe the following capabilities will differentiate leading microsegmentation solutions from legacy approaches?

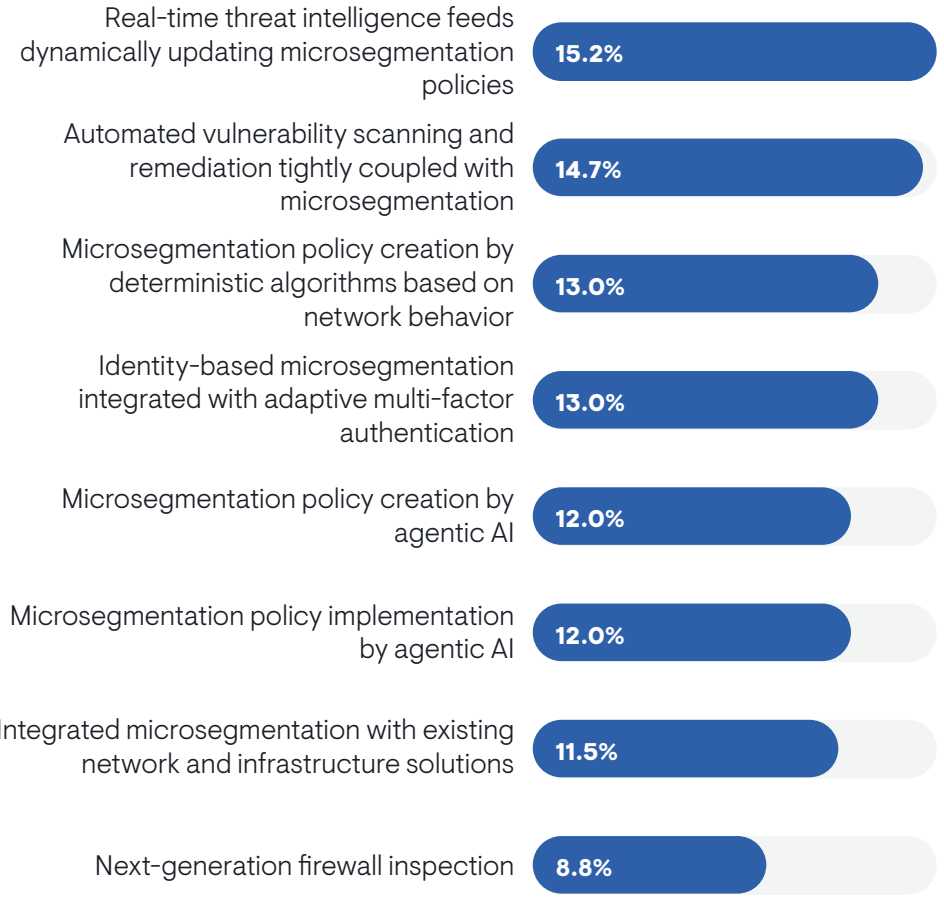


Real-time threat intelligence feeds dynamically updating microsegmentation policies received the highest number of mentions (15.2%) when discussing the perceived effectiveness of various capability combinations in defending against lateral movement and ransomware over the next 1-2 years. This suggests a strong belief in the power of proactive, intelligence-driven security adaptations. Closely following were automated vulnerability scanning and remediation, tightly coupled with microsegmentation (14.7%) and microsegmentation policy creation by deterministic algorithms based on network behavior, along with identity-based microsegmentation integrated with adaptive multi-factor authentication (both 13%).

Microsegmentation policy creation/implementation by agentic AI (both 12%) also garnered attention. Next-generation firewall inspection received the fewest mentions (8.8%), indicating it might be considered less central to a robust defense strategy against these specific threats compared to the other combinations.

Overall, the data emphasizes a future in which a layered approach combining dynamic threat intelligence, automated vulnerability management, behavioral analysis, and strong identity controls is seen as most effective in combating lateral movement and ransomware. The integration of microsegmentation with existing infrastructure and the potential of AI-driven policy management are also recognized as valuable components of this evolving defense landscape.

Which of the following combinations of capabilities do you believe will provide the most effective defense against lateral movement and ransomware in the next 1-2 years?





EMA Perspective

When approaching this research project, EMA wanted to understand if network microsegmentation was not only understood by technical decision-makers and practitioners, but had also gained acceptance as a critical component of a cybersecurity strategy. The data indicates that microsegmentation's primary perceived benefit lies in the ability to instantly quarantine and contain threats, closely followed by halting lateral movement and thwarting ransomware. Also, those polled overwhelmingly consider microsegmentation to be either extremely important or very important for overall cyber defense.

When selecting a modern microsegmentation solution, organizations prioritize automated tagging, policy creation, and enforcement for ease of deployment and management, alongside the core security requirement of preventing ransomware and lateral movement. This highlights a dual focus on operational efficiency and fundamental security efficacy.

Looking ahead, several capabilities are expected to significantly differentiate leading microsegmentation solutions. Automated policy creation and lifecycle management; along with fast, automated asset discovery and tagging; and integration with multi-factor authentication for privileged access are all deemed critically important. This vision emphasizes the need for intelligent, scalable solutions that minimize manual intervention and enhance the security of the microsegmentation infrastructure itself.

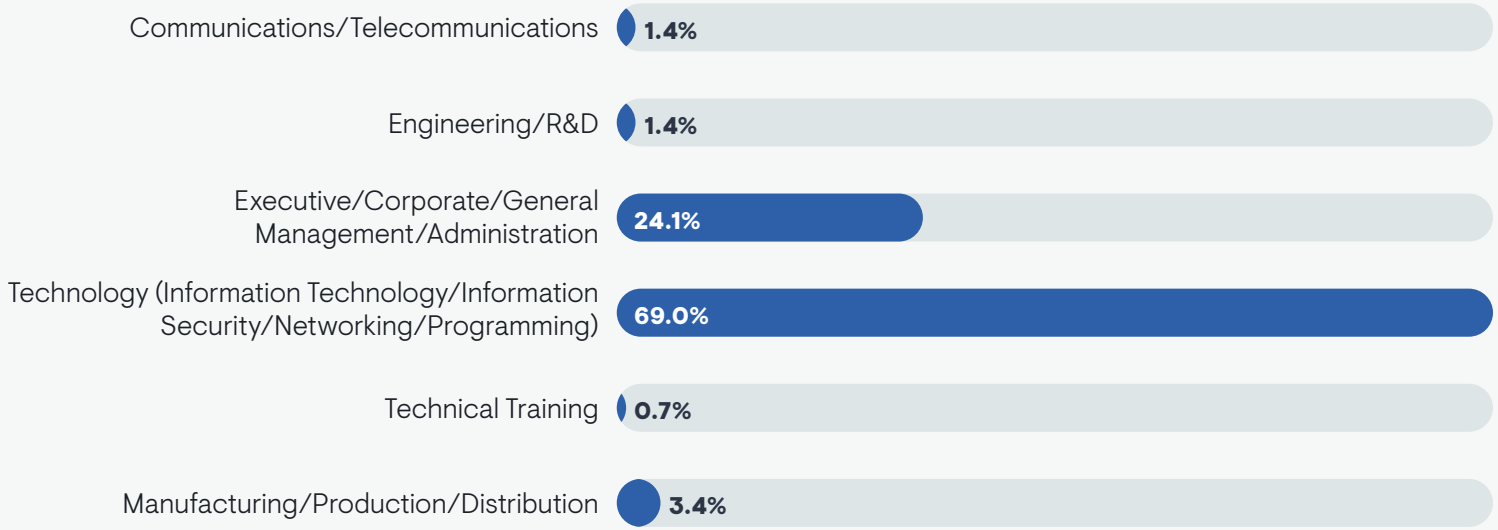
Lastly, the most effective defense against lateral movement and ransomware in the coming years is anticipated to be a combination of several advanced capabilities. Real-time threat intelligence to dynamically update policies, and automated vulnerability scanning and remediation coupled with microsegmentation, are seen as particularly potent. The integration of microsegmentation with existing infrastructure, AI-driven policy management, behavioral analysis, and strong identity controls are also considered vital components of a robust future security posture.

From this data, a clear perspective emerges: microsegmentation is no longer viewed as a niche security technology, but as a foundational element of modern cyber defense. Its immediate benefits in threat containment are highly valued, and its future evolution is expected to be driven by intelligent automation, identity-aware and informed policy creation, seamless integration with existing security tools, and a proactive, threat-informed approach. Organizations are seeking solutions that not only enhance their security posture against sophisticated attacks, like ransomware and lateral movement, but also simplify the complexities of deployment and ongoing management in increasingly dynamic and hybrid environments. The emphasis on real-time intelligence and automated remediation signals a move toward more adaptive and resilient security architectures built upon a strong microsegmentation foundation.

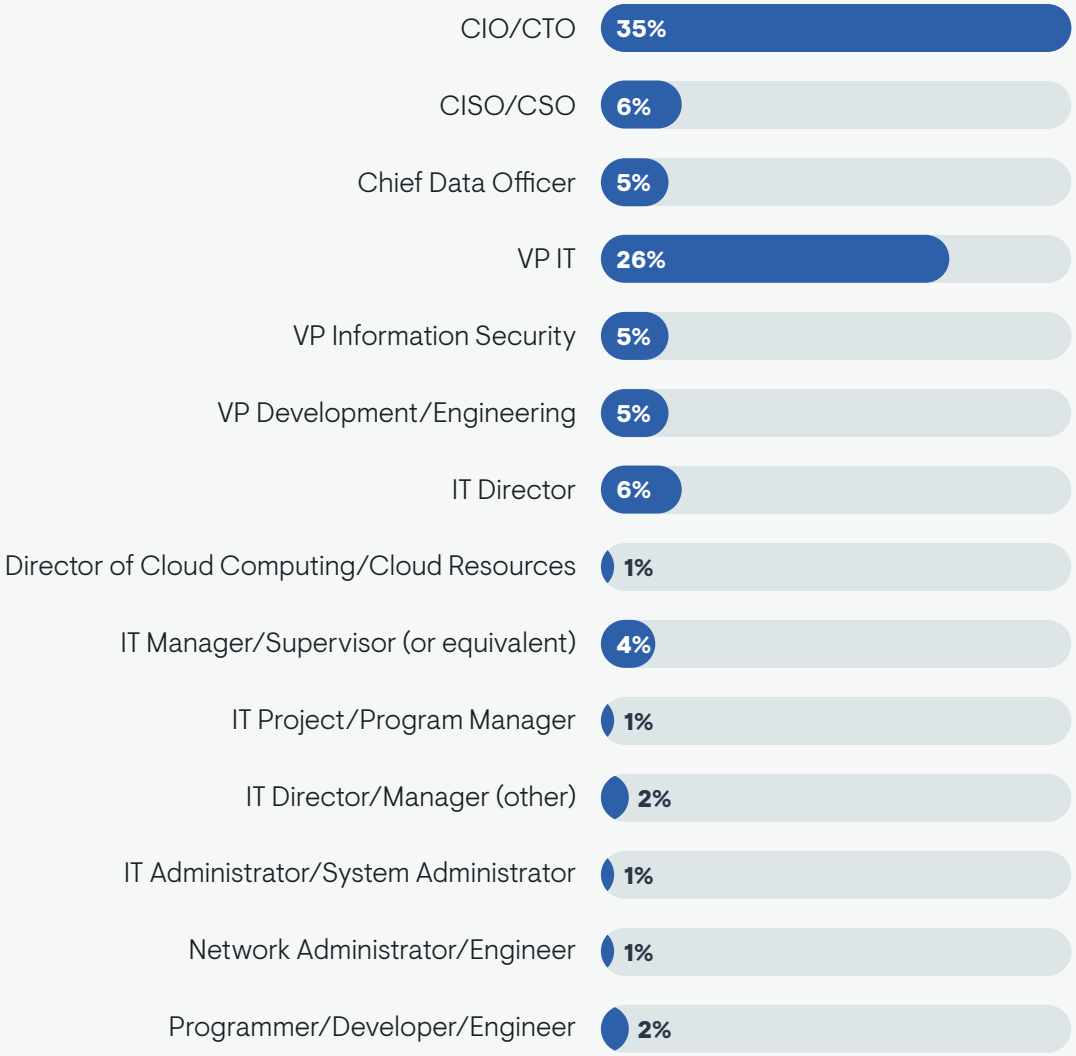


Research Methodologies and Demographics

Which of the following best describes the department or functional area in which you work?

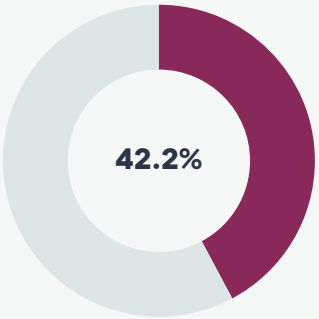


Which of the following BEST describes your specific role?

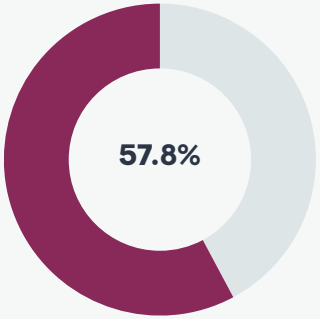


Sample Size = 100

Corporate/Line of Business Vice President (VP/AVP/SVP/EVP)

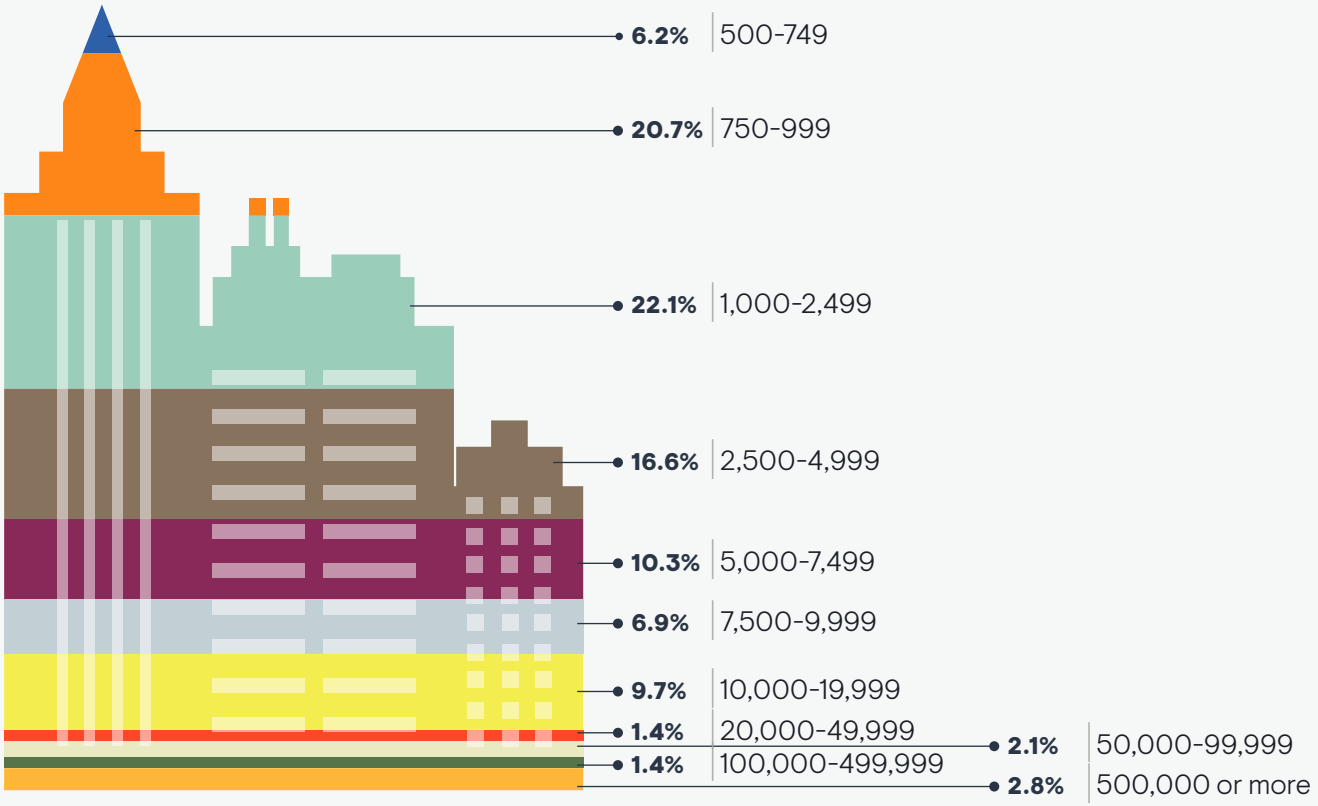


Corporate/Line of Business CEO/President/Board of Directors

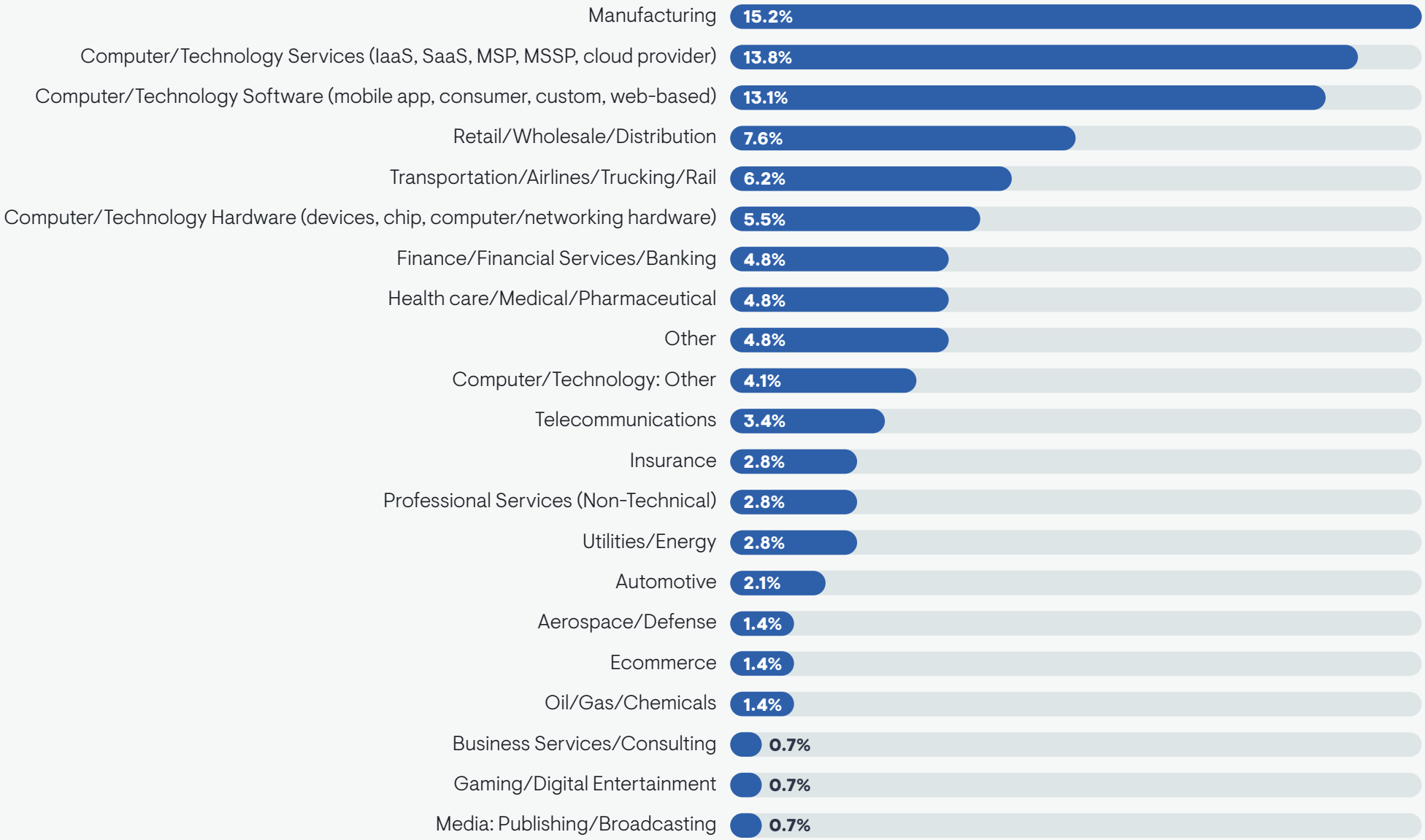


Sample Size = 45

In total, how many employees are currently working in your organization?



Which of the following best describes your organization's primary industry?

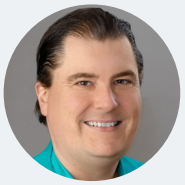




EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING



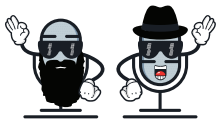
Christopher M. Steffen, CISSP, CISA
Vice President of Research
CSteffen@enterprisemanagement.com



Ken Buckler, CASP
Research Director
KBuckler@enterprisemanagement.com

Check out the CyberSecurity Awesomeness Podcast:
https://www.cybersecurityawesomeness.com

CYBERSECURITY
AWESOMENESS PODCAST



EMA



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**.

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.

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

4548.061125