

2022 State of API Security

May 2022 EMA Research Report

Christopher M. Steffen, CISSP, CISA

Managing Research Director, Information Security, Risk and Compliance Management





Table of Contents	1	Introduction
	3	Key Findings
	5	Voices of the Survey – Respondent Quotes
	7	Technology Trends
	10	Shining a Light on the State of API Security
	15	EMA Perspective
	17	Research Methodologies and Demographics



Introduction

For years, security vendors have discussed DevSecOps solutions and the benefits they bring to the mature enterprise, but 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. Modern applications, composed of functions and services, require developers to rely on APIs to communicate between applications and their components to share data and drive functionality. These applications are mobile, distributed, and have instances in cloud and on-premises.

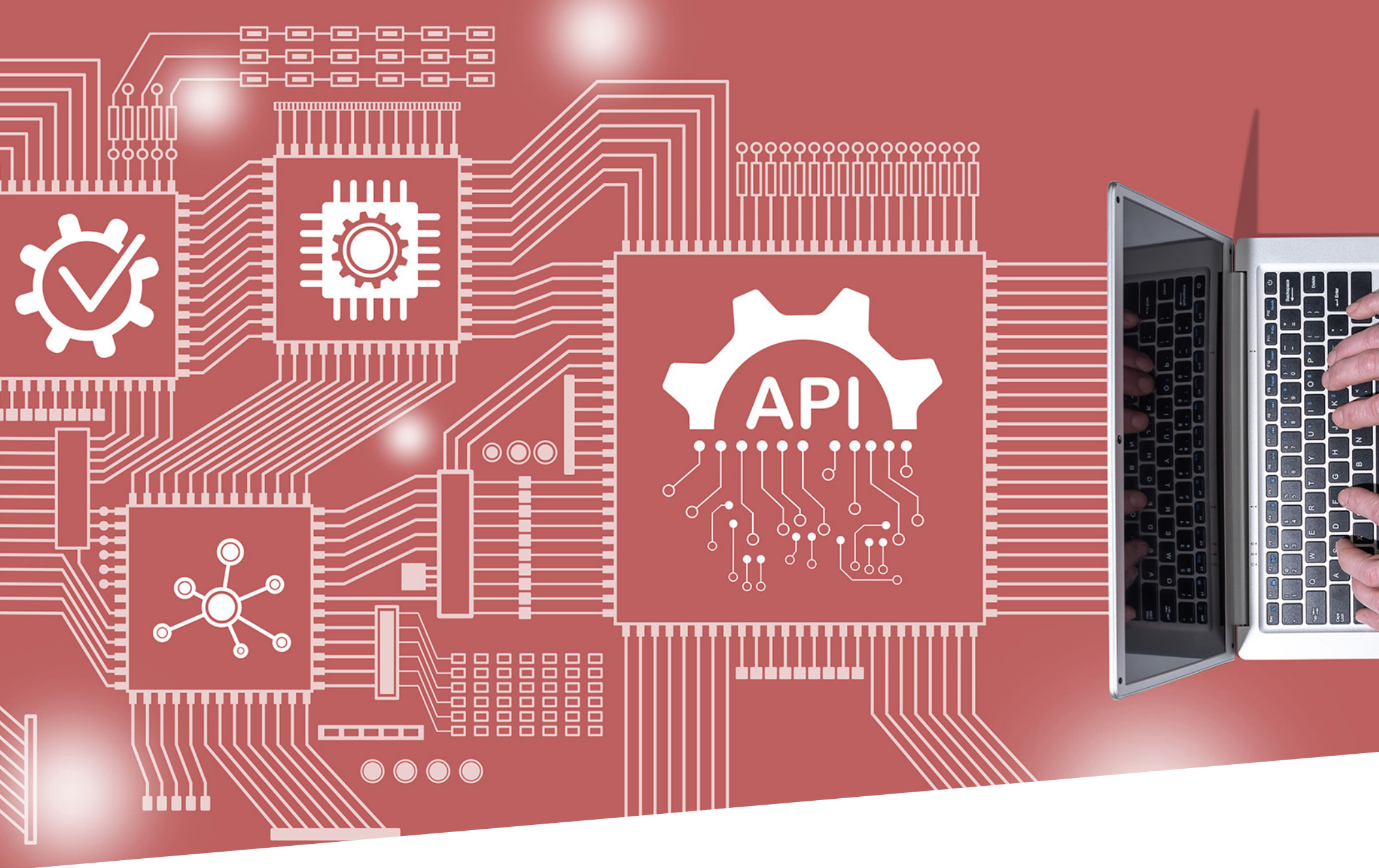
The trend of remote working has created a need for agile, connected applications and deprioritized on-premises application access. This is driving network and application re-architecture, as well as adoption and transitions to cloud while increasing the use of open APIs in many vertical industries. For most organizations, gaining a consolidated view of their configuration and security parameters is challenging because many of these applications are deployed in

a variety of platforms, change frequently, and may include open-source components. Also, due to constant and rapid changes, many of these applications are poorly documented, with API security often becoming an afterthought.

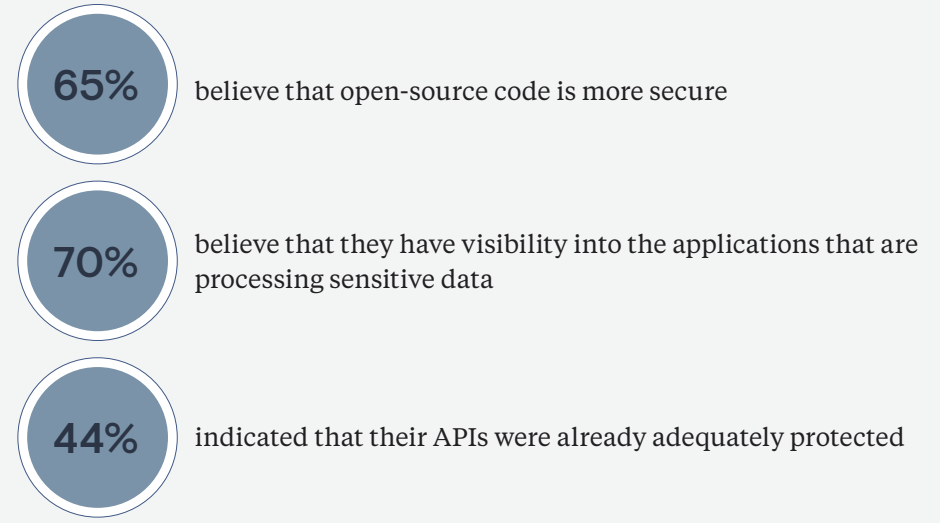
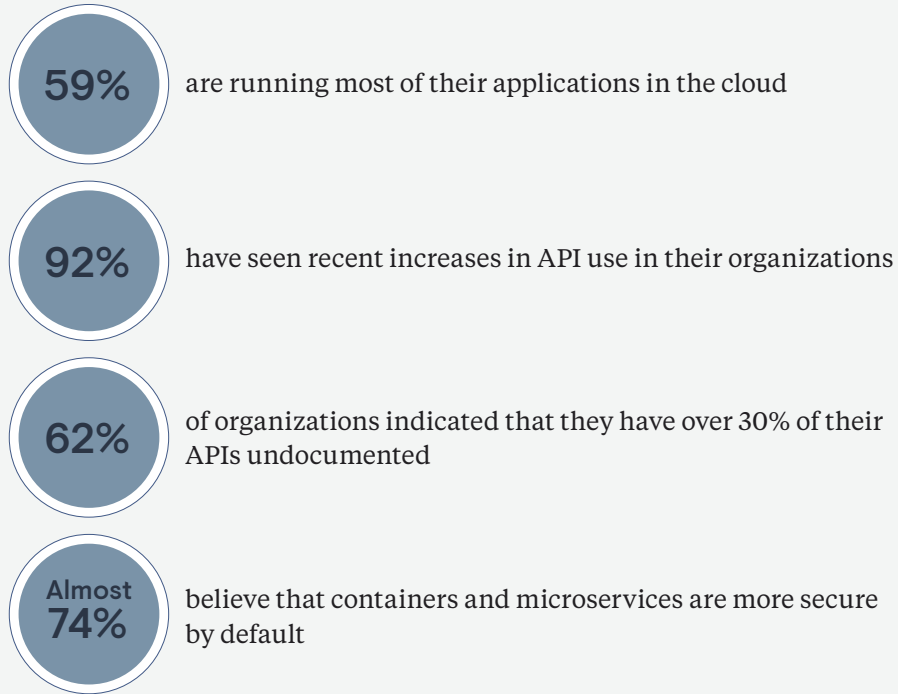
This report examines the state of API security in the enterprise, from how enterprises are evaluating and using tools for API security to the approaches that organizations are taking to secure their applications and APIs. It will also shed light on the false sense of security that many organizations have regarding APIs, specifically how they are documented, how they are used, and how they are secured.

In this exclusive research study conducted for Radware, Enterprise Management Associates polled 203 individuals in Europe, Asia, and North America, representing organizations of 1,000 employees or more from more than ten different industry verticals. Nearly all (96.6%) indicated that their organization is utilizing APIs for communications between their workloads and systems, and 92.6% stated that they have a plan in place to protect those APIs from being exploited.





Key Findings








Voices of the Survey – Respondent Quotes


Select Open-Ended Responses


Why is securing your organization's API important to your business?

“
 For our company, API security is essential because it allows for more rapid innovation and API to make our monetization simpler. Our company will be able to sell more advertising space. A good example of this Uber, which took the finest features of all these program and linked them together through APIs.
”

“
 We operate in an era in which more actions are being done online than ever before. Customers trust us with sensitive information, and we owe it to them to protect their data with the most stringent and latest security features.
”

“
 As a financial institution, we deal with very sensitive data and customer information. Most of our due diligence has copies of personal ID and social security numbers. Therefore, most of the data is stored in an electronic format on cloud servers and its crucial API is well maintained.
”

“
 API security is important ensure safe connection of IT services and to transfer data, without any breaches.
”

“
 It allows for faster innovation of our services. It removes barriers to change, and we can create better services while standing apart from the competition.
”

“
 They enable our line of business users and information technology to use application and software to increase productivity and improve the bottom line of the organization. Therefore, APIs is extremely important in our business.
”



Technology Trends

Analysis:

When starting with a survey of this type, it is always important to ask some baseline questions to get a sense of how the respondents view the topic. In this instance, 96.6% of the respondents are using APIs in their organizations for connections between their workloads, and 89.2% have some level of responsibility for securing those APIs.

Commentary:

This question and data alone suggest the reason for the survey: APIs are critically important for nearly all organizations, and securing those APIs from attack or exploit is the responsibility of nearly 90% of those surveyed.

Does your organization use application programming interfaces (APIs) for connections between computers or computer programs?



Are you responsible for API security within your organization?



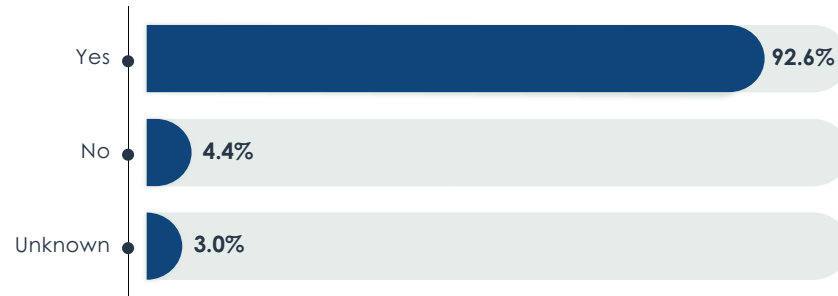
Analysis:

API usage is up, and the organizations surveyed believe that they have a plan to address their protection. Over 92% of those surveyed indicated that their API usage had increased significantly or somewhat, and the same number (92%) believe that they have a plan in place to adequately protect those APIs from attacks.

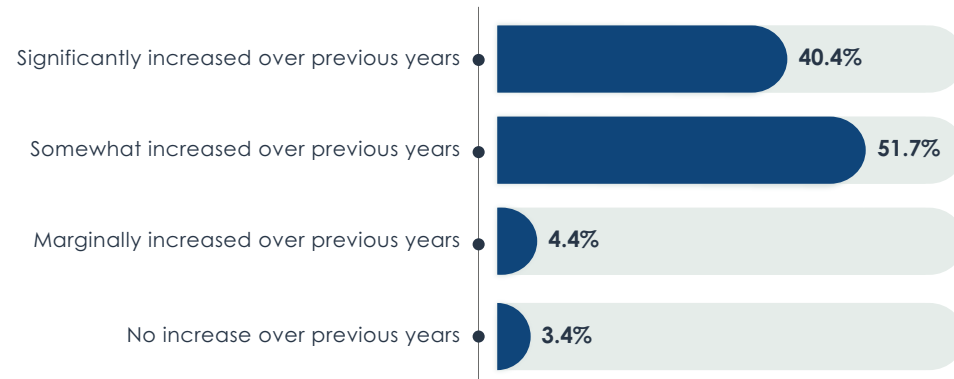
Commentary:

It is not surprising that API usage is increasing. The proliferation of applications in the cloud and on mobile devices nearly guarantees that result. Interestingly, those surveyed believe that they have the ability – and visibility – to protect those APIs from attacks, which is at odds with some of the other data from this survey and creates a false sense of security and protection of those applications on critical workloads.

Does your organization have a plan to protect APIs utilized by your applications?



How has API use increased in your organization compared to previous years?





Shining a Light on the State of API Security

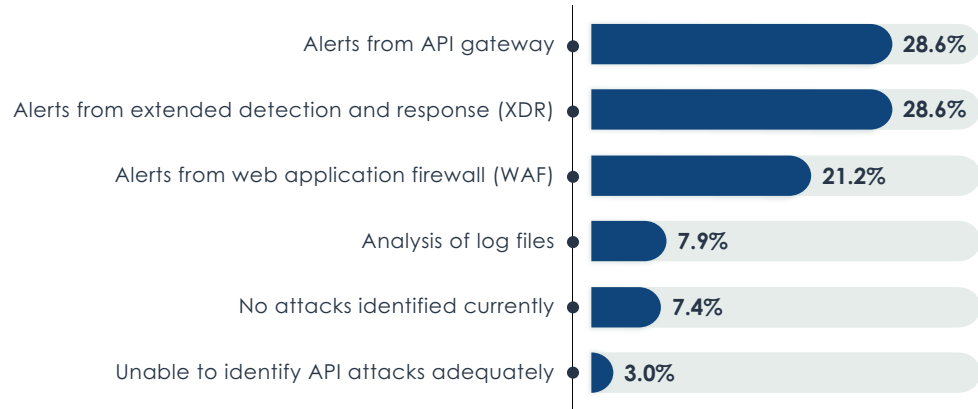
Analysis:

When considering the methods used to identify and protect APIs from attack, many of the standard solutions are referenced: XDR (29%), API gateways (29%), and web app firewalls (21%). Also interesting was the idea that these solutions were nearly 98% effective at protecting their APIs.

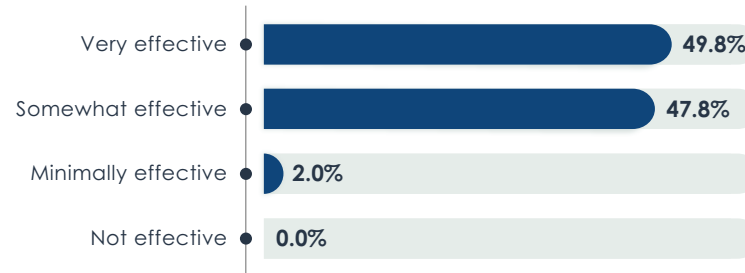
Commentary:

Maybe the most troubling response from these two questions was that the solutions in place did not identify attacks (7.4%). There was also the honest assessment that the tools deployed were not able to adequately identify API attacks (3%), but also call into question whether the existing tools are delivering a false impression that they are adequately identifying when API attacks occur. It seems unlikely that the solutions referenced are 98% effective, especially when over 7% of those surveyed indicate that there were no attacks to identify.

What is the PRIMARY method currently used by your organization to identify an attack on your APIs?



How effective are your existing tools in protecting your APIs?



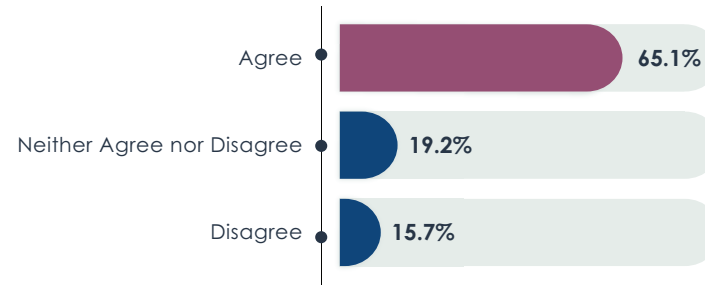
Analysis:

Further contributing to the false narrative is the concept that open-source code and microservices are inherently more secure. In this survey, 65% of respondents believe that open-source code was more secure and nearly 74% believe that containers and microservices are more secure by default.

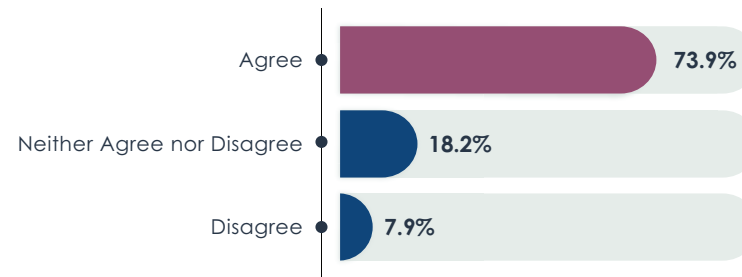
Commentary:

In general, the security industry tries to scare customers and prospects into thinking that the sky is falling, while other technologies will tell you everything is just fine. That must be the case here, since open-source code is not the magic bullet to development security. It consistently has the same security concerns and flaws that proprietary code has and is usually patched much in the same way. Same with containers and microservices: they are vulnerable to many of the same exploits that cloud instances and traditional servers are subject to. Believing that these technologies are inherently more secure contributes to the false narrative that puts application security and organizations at risk to cyber-attack.

**Please rate the following statement:
Open-source code is more secure since the community constantly improves and patches it.**



**Please rate the following statement:
Containers and microservices are more secure by default.**



Analysis:

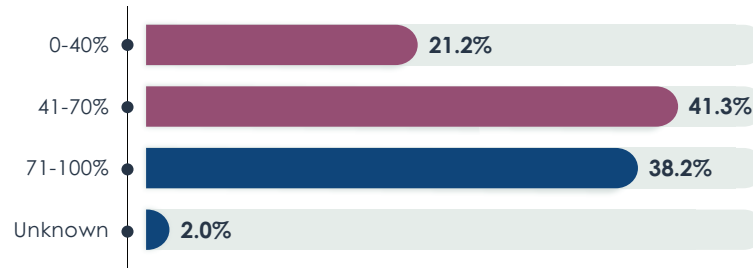
Arguably, you can't protect the things you don't know you have. In this survey, only 38% indicated that they had documented at least 70% of their APIs. In other words, 62% of organizations surveyed have 70% or less of their APIs documented. In response, those surveyed realized that a good solution for API protection needs to discover and secure undocumented APIs, as well as reduce the security skill necessary to protect APIs wherever they might be in their various environments.

Commentary:

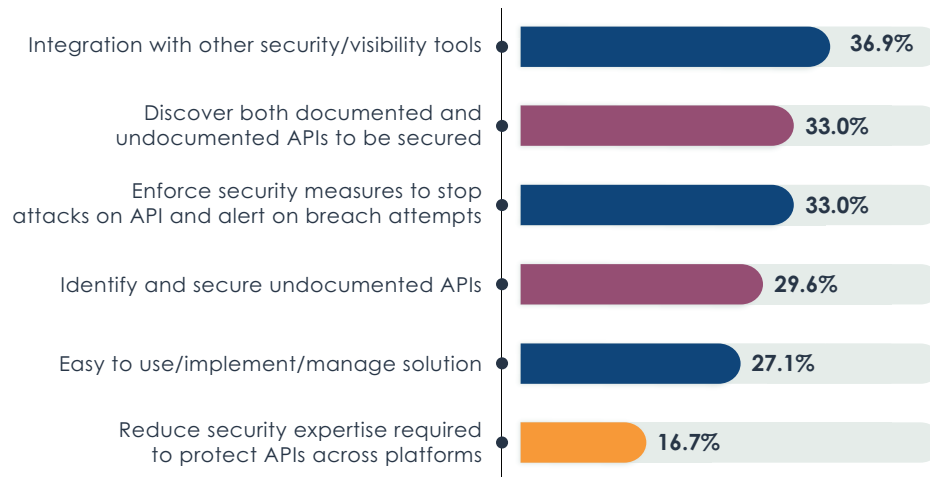
Again, the data is very consistent: organizations are aware of the process shortcomings in their dev and operations cycles regarding documentation of application APIs and are looking for solutions to address those shortcomings. They are obviously looking for tools that integrate with existing solutions and ones that can enforce security policies, as they should. Still, finding ways to detect and secure APIs that are documented and APIs that are undocumented is a key feature that organizations are looking for when selecting their API security tools.

It is also critical to find solutions and tools that allow organizations to easily protect their APIs regardless of their location. Any tool that requires an entire security team to administer is not going to be a viable tool to protect APIs in most organizations, as they lack the skills and manpower to dedicate to API protection – they are depending on the tool and vendor to aid them with this process.

In your organization, what percentage of APIs are documented?



What do you perceive to be a good solution to protect APIs?



Analysis:

The ability to address automated or bot attacks is one of the concerns that was top of mind for respondents on the survey. Nearly thirty-two percent indicated that bot attacks is the most common threat they are seeing against their APIs. While not the most mentioned threat, it is much greater than it may seem due to the data breach indicators of the threats that were more frequently mentioned.

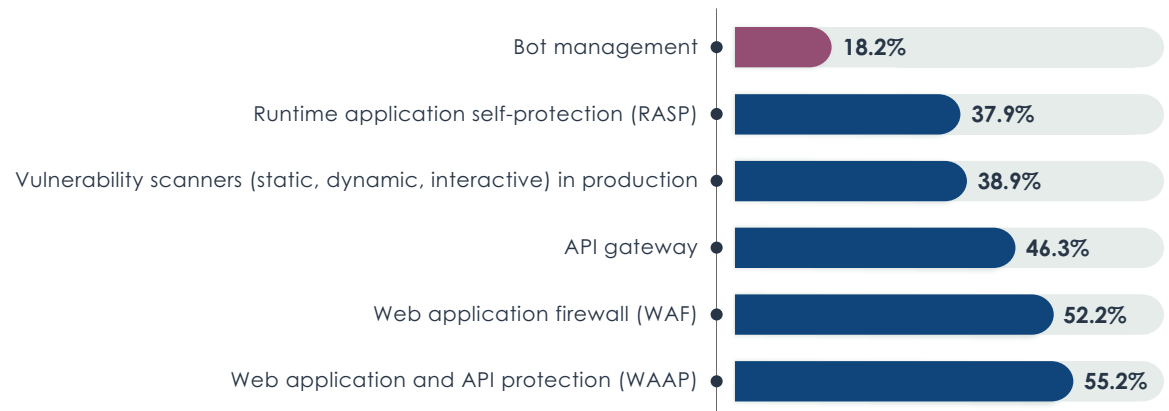
Commentary:

Bot mitigation arguably solves one of the most significant threats to an organization’s APIs. Yes, companies need solutions for WAAP, WAF, and API gateways, but often, bot mitigation is overlooked as a critical component. Most comprehensive application protection solutions have remedial bot mitigation protection as part of their overall protection suite of tools, but bot protection/automated attack protection should be a priority when evaluating tools/solutions to protect APIs.

What are the most common threats you've seen on your APIs?



What tools does your organization use to protect APIs?





EMA Perspective

More than most of the verticals in the technology space, the security industry (more specifically, the marketing and media around the security industry) is all about the latest trends. Be it Zero Trust, the latest ransomware attacks, or whatever data breach is the latest in the 9:00 o'clock news, executive leadership of organizations of every size react to these trends, forcing the vendors in the space to react as well. API security is one of these trends, but one that has received very little attention to date – and has led many organizations to embrace a false narrative that their APIs are secure (if it isn't being reported on CNN, it must be secure, right?). Put simply, there is a false sense of security and over confidence when it comes to API protection, stemming from a multitude of sources: the belief that open-source environments are more secure, that auto-discovery tools and solutions have identified and protected undocumented applications and APIs, to the idea that existing tools are adequately protecting APIs against automated and bot threats.

In reality, there are many challenges in securing APIs in their environments, including:

- Protecting the unknown. While this survey discovered that a fair portion of APIs are known and documented, there is a real (and underestimated) threat that comes from a large percentage of undocumented APIs. This is coupled with the fact that only some people believe that automatic API discovery and protection are necessities, and a smaller portion is actually using a solution with such autodiscovery capabilities. This is part of the false narrative that can lead to disaster for many organizations: the belief that they are adequately protected, but actually have significant gaps in their protection from APIs that are unknown and undocumented.
- Overconfidence. Throughout the survey, there were plenty of instances in which respondents thought they had adequate protection for the environment with their existing tools and solutions, only to find that they did not have solutions that address a majority of the most common threats. **For example, there is a false belief in the adequacy of API gateways and traditional WAFs providing adequate protection of APIs against both vulnerability and automated bot exploits, but that is simply not the case.** A comprehensive API protection solution will address these threats, but very few respondents indicated that they had solutions that actually did, or even had the capability to do so.

- Overcoming the skills/talent gap. A reoccurring theme in the security space is the lack of security talent. Even the most experienced security administrator may not have the development skills necessary to architect and deploy a best-in-class security strategy for protecting APIs and application workloads. Protecting APIs is not a simple task – it requires in-depth understanding of a multitude of environments and platforms. Often, the only recourse for protecting these environments is to partner with a trusted vendor with experience in the processes and solutions needed to protect the APIs in these environments.

There is unequivocally a false sense of over confidence when it comes to API protection, but there are solutions that exist to secure these resources. From our perspective, an API security solution will have most of the following capabilities:

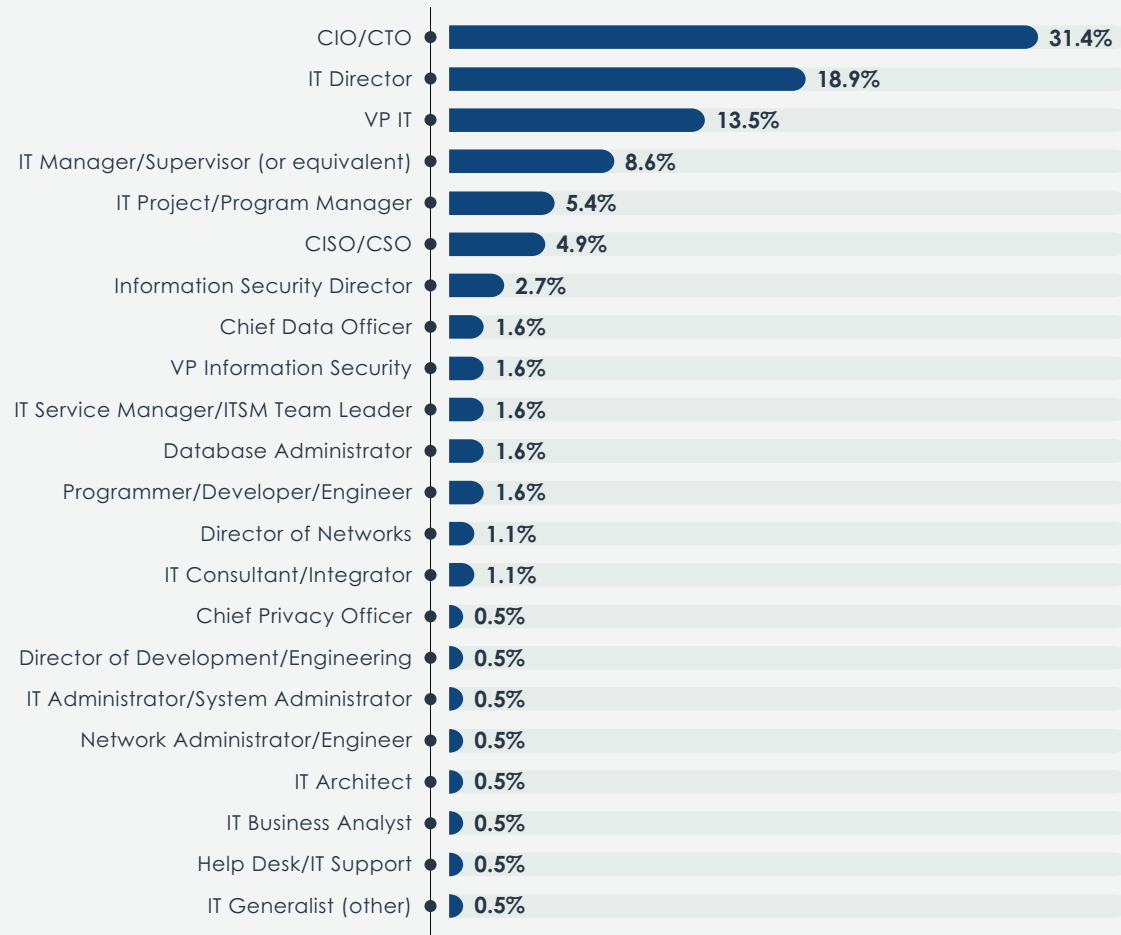
- The ability to integrate well with existing security and visibility tools in the environment
- Reduces security and deployment expertise and resources (manpower) required to protect APIs across platforms
- Leverages advanced machine-learning algorithms to detect emerging threats and automatically creates and optimizes API security policies
- Enables accurate and automated API discovery, protection and security policy generation without requiring application or security expertise
- Provides comprehensive API protection of all parts of the API and across a broad range of API threats such as:
 - access violations
 - data leakage
 - denial of service
 - automated threats (bots)
 - embedded attacks
- Protects API against automated, bot-based threats
- Supports both positive and negative security models while enabling continuous and automatic security policy optimization and adjustments to correct and eliminate false positive events

API security is not a “trend” that is going away. APIs are a fundamental component to most of the current technologies, and securing them must be a priority for every organization. Dispelling the myths and false beliefs while debunking the over confidence that most organizations have around API security is a great place to start, and working with a vendor that debunks some of these false beliefs is critical.



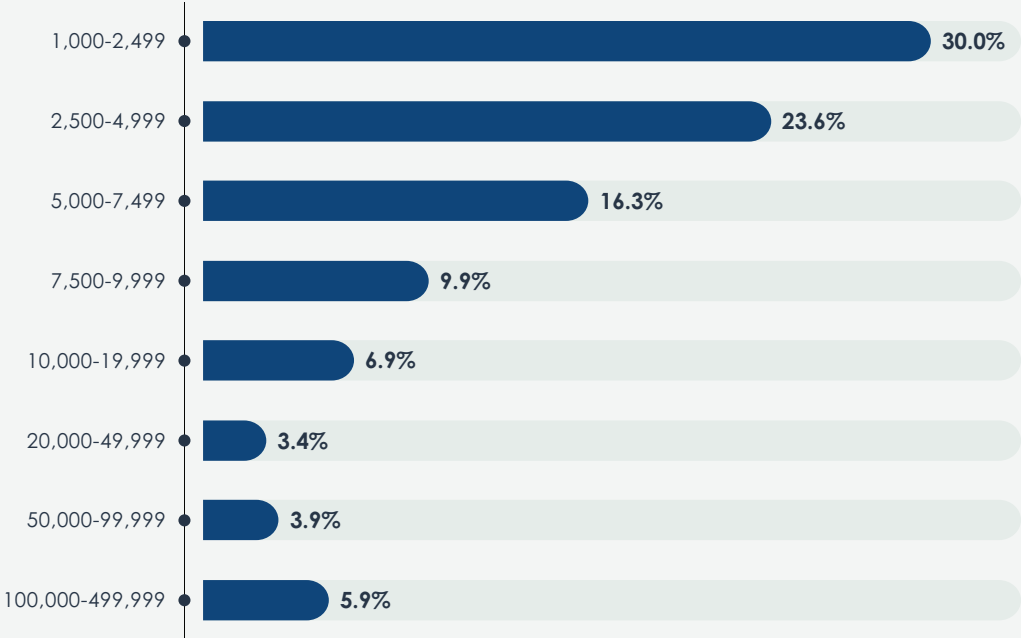
Research Methodologies and Demographics

**You indicated that your department is IT-related.
Which of the following BEST describes your specific role?**



Sample Size = 203

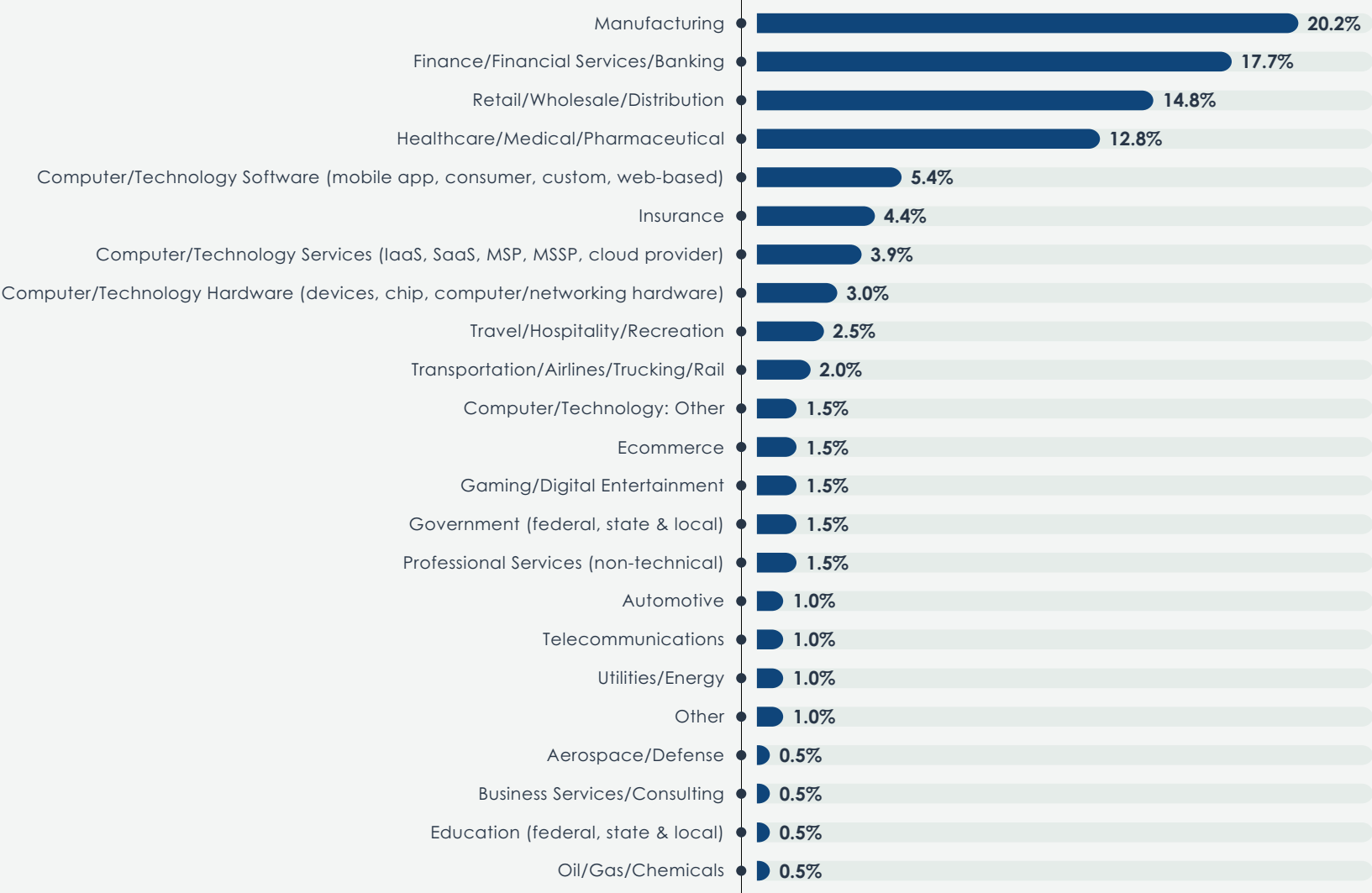
In total, how many employees are currently working in your organization?



In which region is your organization's headquarters located?



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







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](#).

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.

©2022 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.