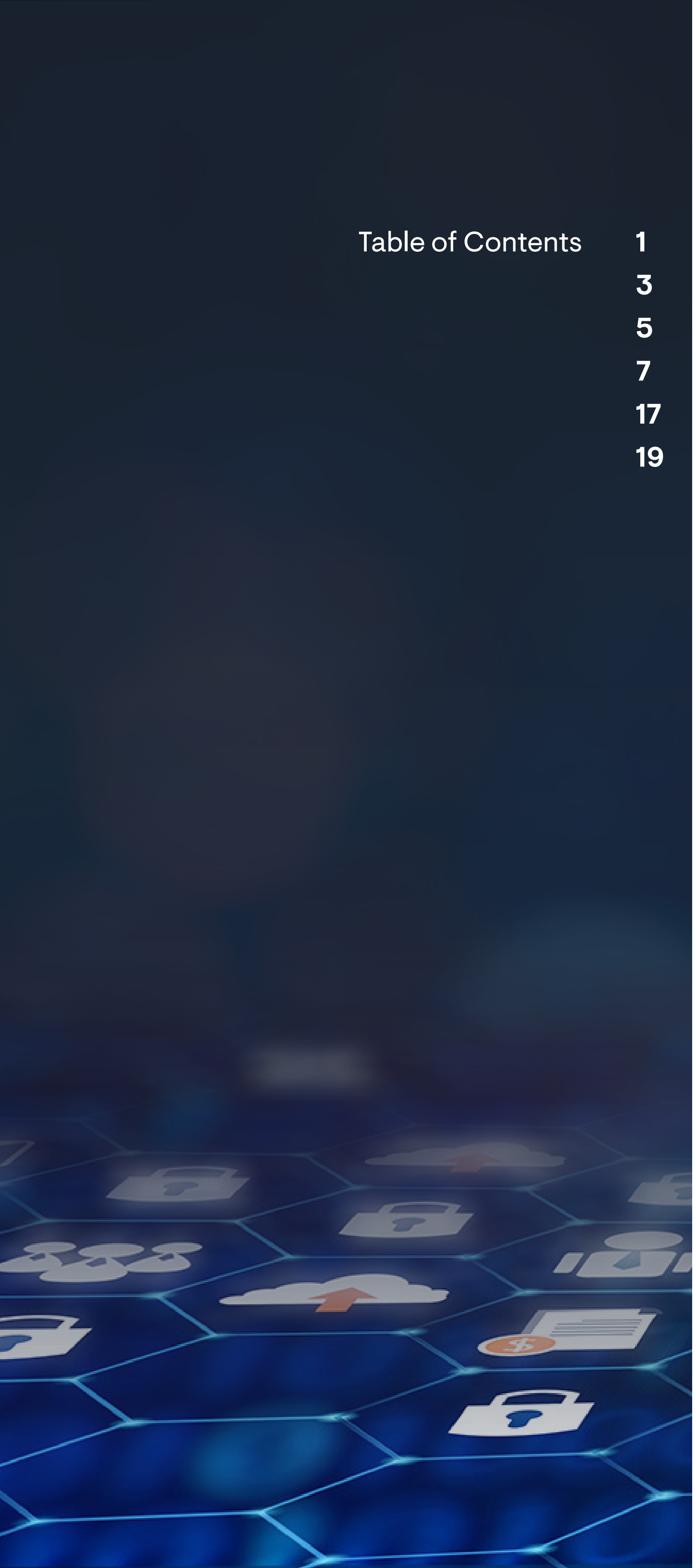
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

# API Security: Debunking the Myths

**March 2023 EMA Research Report**

**Christopher M. Steffen, CISSP, CISA**, Managing Research Director and **Ken Buckler, CASP**, Research Analyst
*Information Security, Risk and Compliance Management*



## Table of Contents

# Introduction

Enterprises are finally starting to pay attention to application security as theoretical threats to their application infrastructure become reality. 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 are investing in application security tools, and tools that address every market of every size will have a decisive advantage to exploit this emerging trend. As application security teams and development organizations pivot to address these new risks, this research will seek to measure how far enterprises have come in protecting APIs, uncover the challenges they face in trying to secure APIs, and look at strategies that are in place and are being formulated to defend against these new types of threats.

In this research study, Enterprise Management Associates surveyed IT professionals, information security practitioners, and technology business leaders across all verticals to discover their attitudes and perspectives toward API security. It also explored the tools they are using/evaluating to protect their critical workloads.

EMA polled 229 technology and business leaders in North America, representing organizations from more than one dozen different industry verticals and of nearly every size to gain an understanding of their views on APIs and the security surrounding them.

Unlike any study that we previously conducted, the results were shockingly inconsistent—almost to the point that we rejected them as false data. Upon further examination, we found that not only were the responses valid, but they showed a remarkable disconnect between the perception and the reality of the security that the respondents' organizations used for the APIs.

for(s=0; s<=hexagonSize-r; s++){
printf(" ");
int main()
int age;
int year_of_birth;
time_t t = time(NULL);
struct tm tm = *localtime(&t);
int current_year = (tm.tm_year + 1900) + 543;
printf(" Enter your year of birth (B.E.): ");
scanf("%d", &year_of_birth);
age = current_year - year_of_birth;
printf("\n Your age is %d\n", age);
return 0;

# Key Findings

**52%** believe that IT is responsible for API security in their organization

**93%** indicated that they had some role in or responsibility for API security within their organization

**53%** believe their management understands the importance of API security

**97%** have a plan to protect the APIs in use

**46%** believe that their APIs are already adequately protected

**75%** believe that their organization already has a mature API security solution and strategy

**91%** indicated that at least 80% of their APIs were exposed to the internet

**41%** stated that fewer than 50% of their APIs were documented

**82%** indicated that their APIs followed a standard or schema

**5.2%** stated that they use NO tools to document or protect their APIs

**32%** stated that API controls are first implemented in production

**83%** believe that they would know if their APIs were being abused today

**87%** stated that they have API security expertise already in their organization

**95%** believe that their existing tools are effective at protecting their APIs

# Voices of the Survey – Respondent Quotes

# Select Open-Ended Responses: Describe why securing your organization's API is important to your business.

> Securing our API is important so confidential and trusted information can be sent securely. It gives us peace of mind when the messages are in transit through encryption. It also validates and authenticates the data being sent. By accepting queries sent over a secure channel, we maintain production and efficiency without the risk of a breach.

> Securing our organization's API is important because it helps protect sensitive data, maintain customer trust and reputation, ensure legal compliance, and maintain a competitive advantage. Our executive has made securing my organization's API the highest priority and is putting others on hold to achieve that objective. My organization receives and sends files to external organizations and governments to meet regulatory and compliance requirements.

> Securing our APIs is critical to avoid security breaches, as well as remaining in compliance. Right now, many organizations are at risk due to poorly secured APIs and resources, and it is essential to harden services to ensure an organization is protected.

> API security is critical for our business because APIs are used to connect services and transfer data, and a hacked API can result in a data breach since we are working in the mobile software industry. Also, we provide information and technology consultation services, so we put a high focus on secured APIs.

> API security is crucial to our business because it facilitates shielding the facts that are being transferred and stored. When an API is not comfy, it is vulnerable to theft and misuse. Stolen authentication records can be used to get entry to personal facts, control transactions, and damage reputations. This can result in financial losses, prison, and customer dissatisfaction, all of which can have a drastic effect on an enterprise.

> Securing an organization's API is critical for business since it prevents private data from being accessed or abused. Businesses may guarantee that only authorized users can use the API and that the data is safe from bad actors by implementing encryption and authentication mechanisms.

# Research Findings

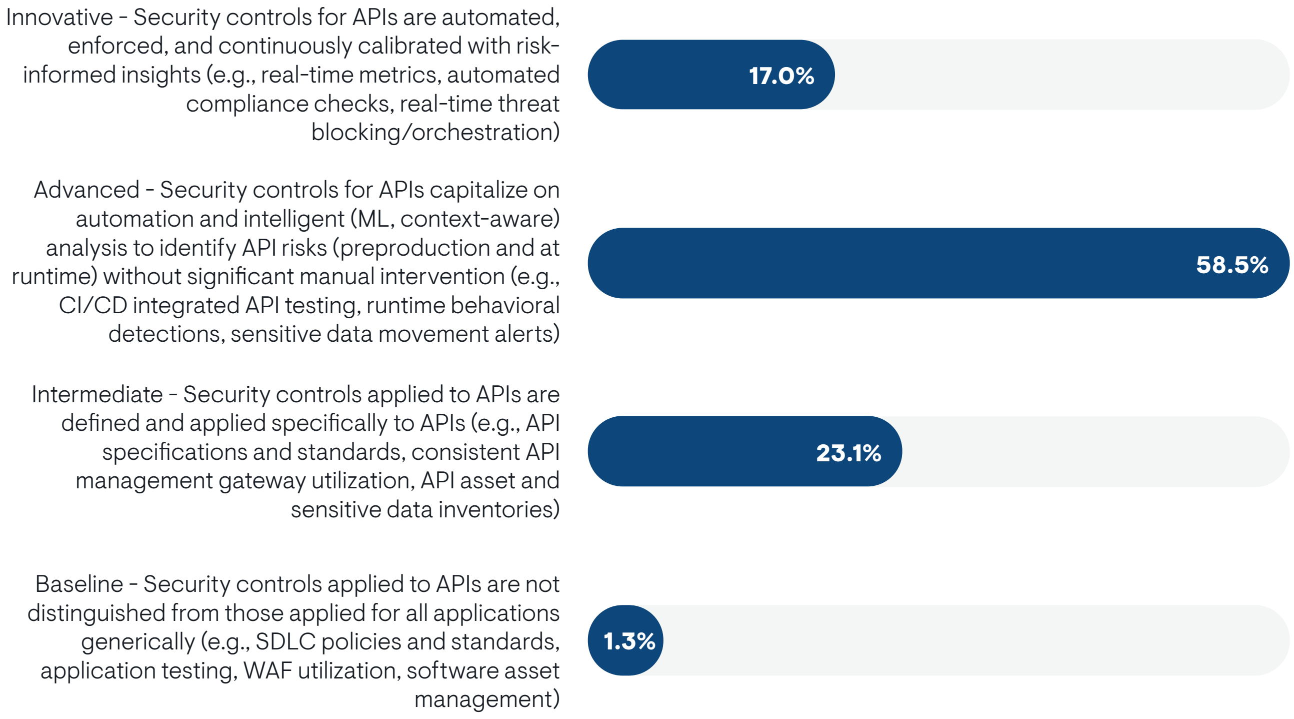
## Analysis:

One of the first questions asked of the respondents was to rate how they viewed their overall maturity regarding API security. Over ¾ (75.5%) rated their maturity as advanced or innovative, believing that they have a strong, demonstrable API security program and strategy. Twenty-three percent believe they have some level of API security, but not advanced, while only 1.3% indicated that they are at a beginning or baseline stage. This directly translates to the feelings/beliefs that are expressed by the organization's leadership in understanding the importance of API security in the organization, with over 90% indicating that they understand or somewhat understand the importance of API security.

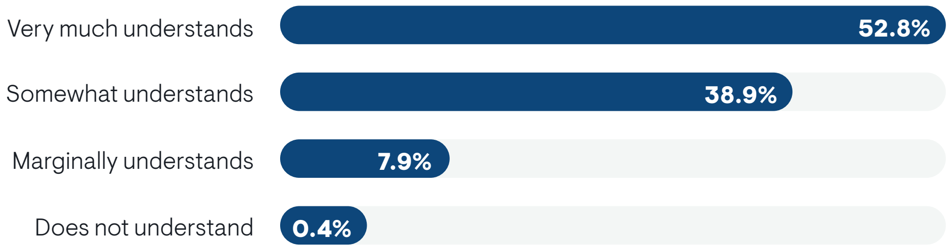
## Commentary:

It is unsurprising (often expected) to rate an organization's security maturity higher than it actually is: we, as humans, security executives, and organizational leaders fundamentally believe that our organizations are more secure than they actually are, regardless of the specific area or topic. When respondents answer that they have a more mature security model applied to their API security, it is in line with what we generally would expect. However, this was not the only area in which organizations had an inflated view of their capabilities. The positive news is that executive leadership is at least aware of the security concerns around APIs, regardless of the actual strength or maturity of their security.

HOW WOULD YOU RATE YOUR ORGANIZATION'S MATURITY RELATIVE TO API SECURITY?



DO YOU FEEL THAT THE EXECUTIVE MANAGEMENT/BOARD OF DIRECTORS OF YOUR ORGANIZATION UNDERSTANDS THE IMPORTANCE OF API SECURITY?



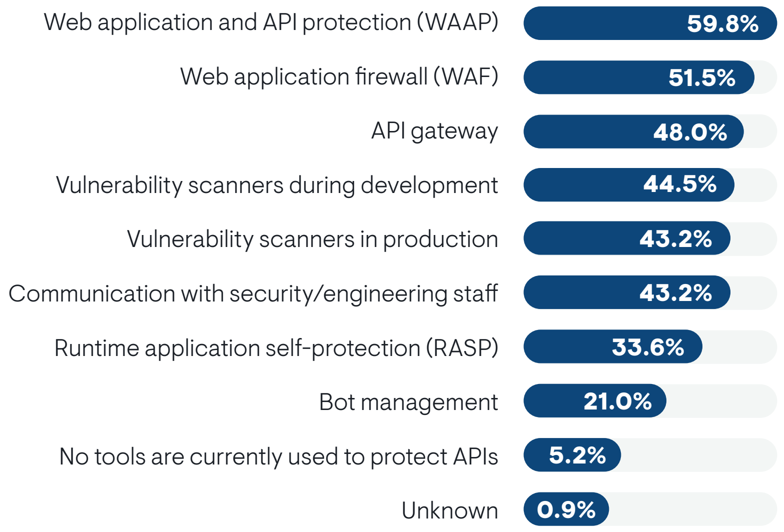
## Analysis:

One of the best ways to determine how mature an API environment might be is to evaluate how well documented the organization's APIs actually are. In this survey, almost 70% of organizations had 30% or more of their APIs undocumented. That speaks only to the APIs that they specifically know about in their environment.

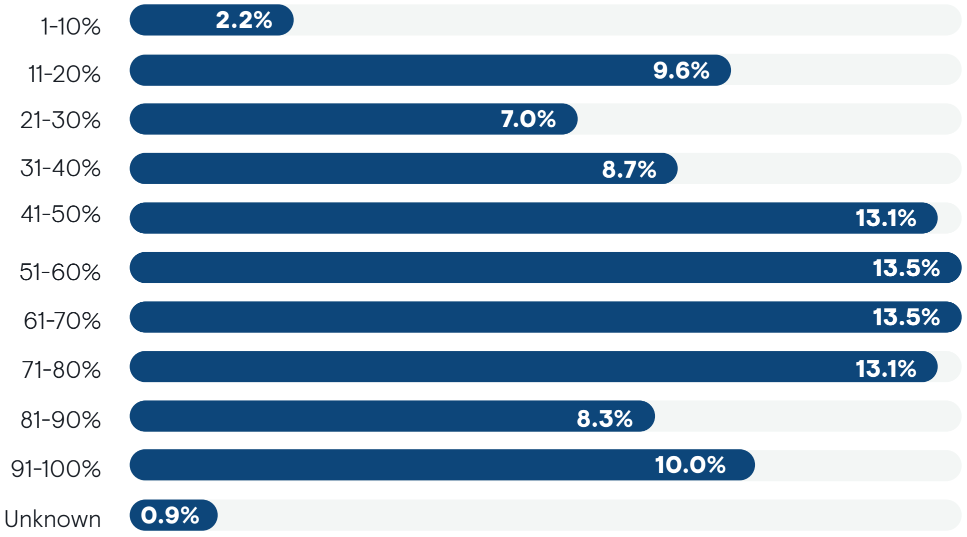
## Commentary:

Developers rarely love documentation, but the quality of the code is directly related to how well the code is documented, as well as how mature the organization actually is with their security and technical processes. In this survey, the fact that over ¼ of an organization's APIs are undocumented (meaning that there is little to no understanding of their function, the data they handle, and possibly even how or what they connect to) is the strongest evidence that organizations that believe they have a "mature" API security strategy have subscribed to a false narrative.

WHAT METHODS DO YOU USE TO DISCOVER/DOCUMENT THE APIS IN YOUR ENVIRONMENT?



HOW MANY APIS ARE DOCUMENTED (PERCENTAGE)?



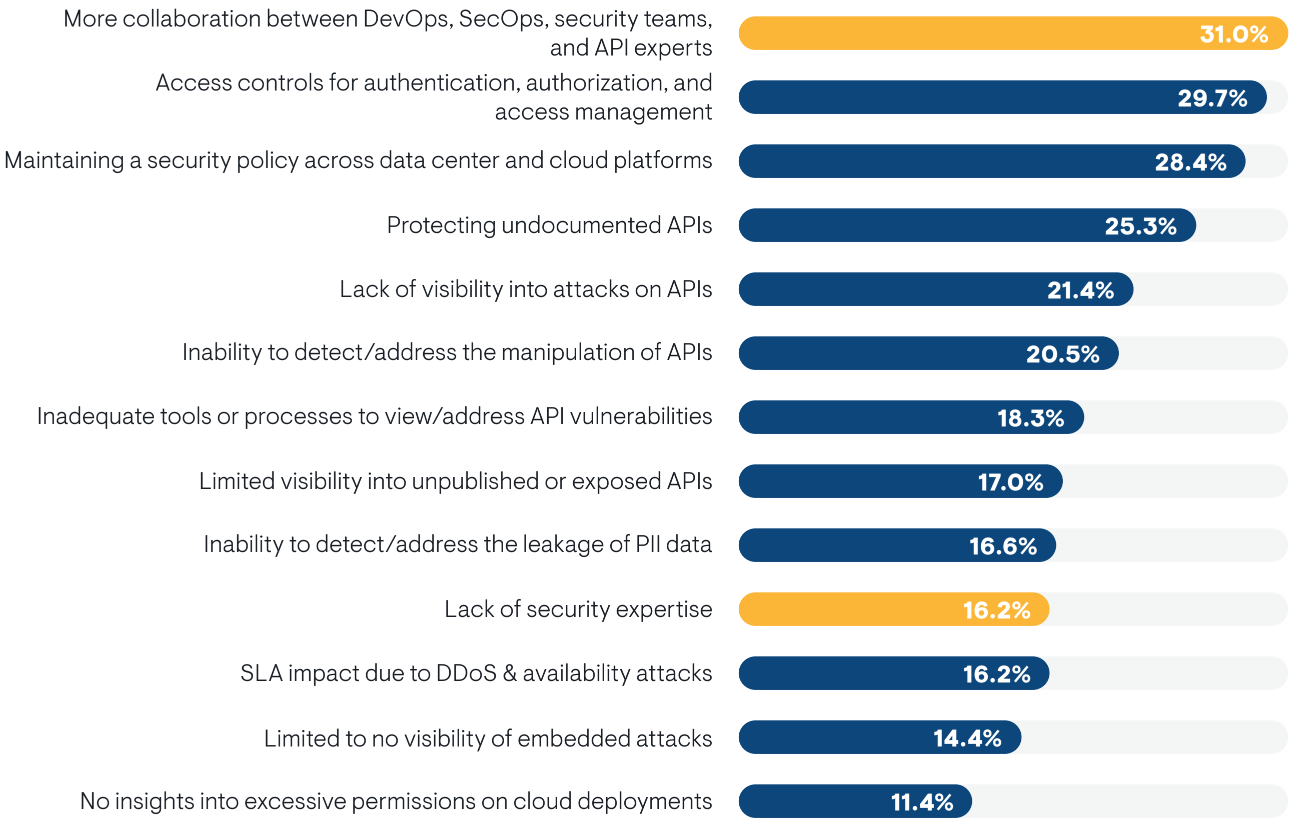
## Analysis:

There are multiple concerns when dealing with API security, but the concern that received the greatest attention was the lack of collaboration between various team with the API security experts. In fact, 87% or organizations claim to have an API security expert available internally. Consistent access controls and a security policy that spans all of the organization's platforms round out the top three concerns.

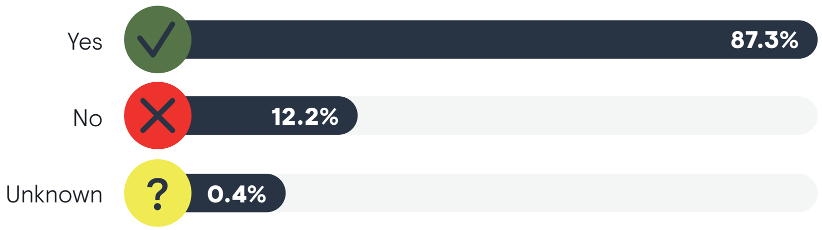
## Commentary:

Breaking down the silos within an organization is difficult regardless of the issue. Security concerns seem to be even more challenging, with many of the silos having competing priorities. In the case of API security, operations, development, IT, and security teams are all at odds with direction and resources regarding how to best approach the APIs the organization uses. Also, while it is reasonable to expect that some organizations have an individual or group that ultimately has oversight into the APIs being used, it is unlikely that a small- to medium-sized enterprise has the resources necessary to retain a viable API security expert. API security experts are a rarity, and while a person might be knowledgeable about some aspects of API development and management, many organizations are falsely reassuring themselves by believing that an individual or group within the organization has the necessary skills to be considered an API security "expert."

IN YOUR ORGANIZATION, WHAT ARE YOUR PRIMARY CONCERNS REGARDING API USAGE?



DO YOU HAVE API SECURITY EXPERTISE INTERNALLY?



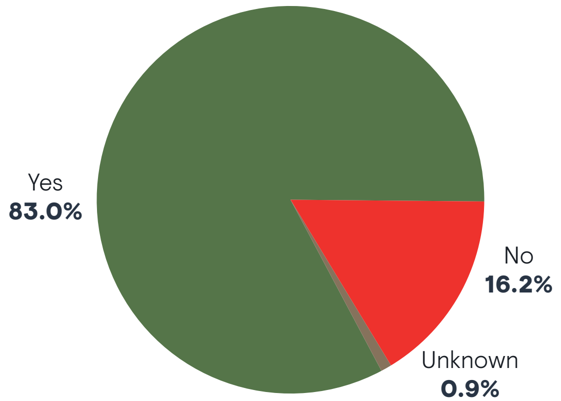
## Analysis:

When asked about the current state of their APIs, 83% indicated that they would know if their systems were being abused or attacked, while 43% indicated that they have a limited ability to effectively protect their APIs using existing security tools.

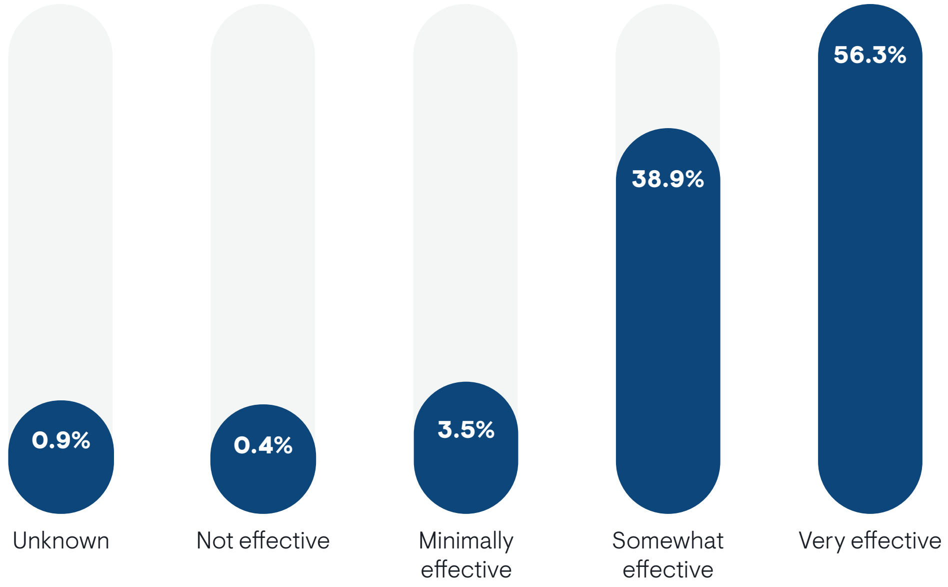
## Commentary:

While it is possible that organizations are using some different tools for API visibility compared to API protection, it seems unlikely that organizations would notice abuse of their APIs and do nothing about it. It is reasonable to infer that the tools organizations are using for API management and security are effective at protecting the APIs that they know about, but can do nothing for the ones where they are lacking visibility. It is also possible that current security tools are not configured correctly to deal with evolving threats, or threat detection solutions and API management/security solutions are not integrated.

WOULD YOU KNOW IF YOUR ORGANIZATION'S APIS WERE BEING ABUSED TODAY?



HOW EFFECTIVE ARE YOUR EXISTING TOOLS IN PROTECTING YOUR APIS?



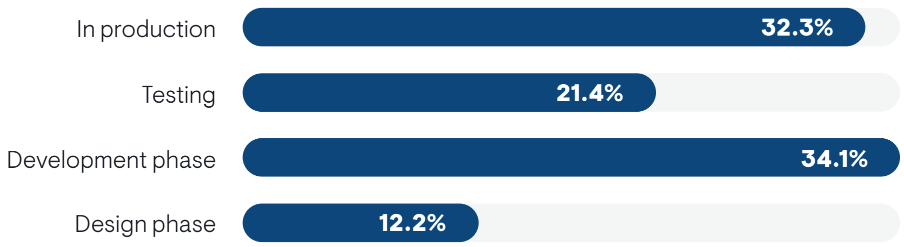
## Analysis:

When asked where the security controls that protect APIs are implemented, 68% stated that it happens in a preproduction phase, such as testing, development, or design. Thirty-two percent promote APIs to a production environment before implementing security controls. Equally concerning is the fact that about one-third (32%) are unsure of the sensitive data that is transmitted via APIs to third parties.

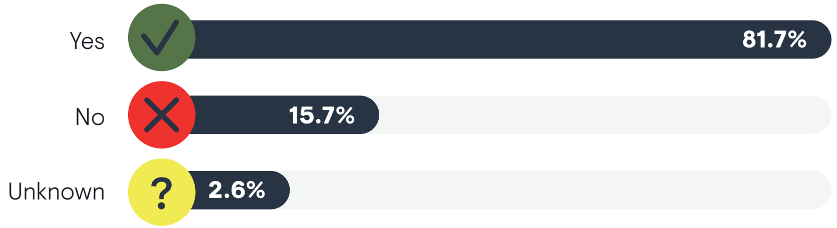
## Commentary:

Ideally, preproduction is the best time to ensure that APIs conform to established standards and security controls. Eighty-two percent of respondents indicated that they follow some kind of API plan or schema, but only 68% implement controls preproduction, a significant statistical variation. It is possible that the API schema has post-design elements for implementation and configuration, but it is more likely a sign that the organization has a schema on paper (for audit/compliance/vendor due diligence purposes) but is not always followed in practice.

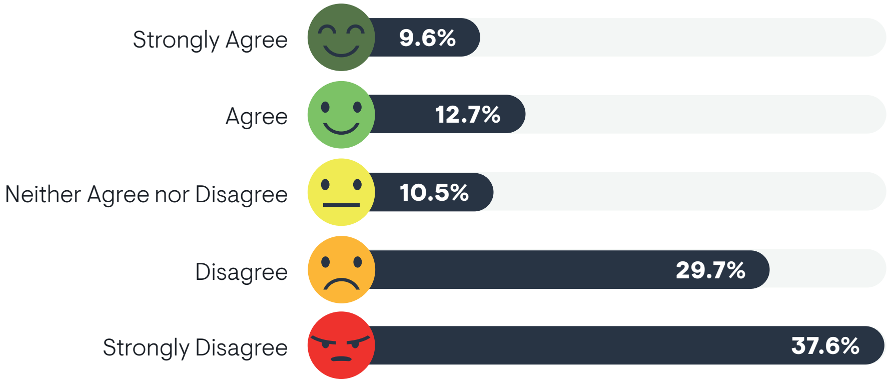
WHEN ARE SECURITY CONTROLS FIRST IMPLEMENTED TO PROTECT APIS?



DOES YOUR ORGANIZATION UTILIZE A DOCUMENTED API SCHEMA?



PLEASE RATE THE FOLLOWING STATEMENT:
I DON'T KNOW IF OUR APPLICATIONS MAKE SENSITIVE DATA AVAILABLE TO THIRD PARTIES



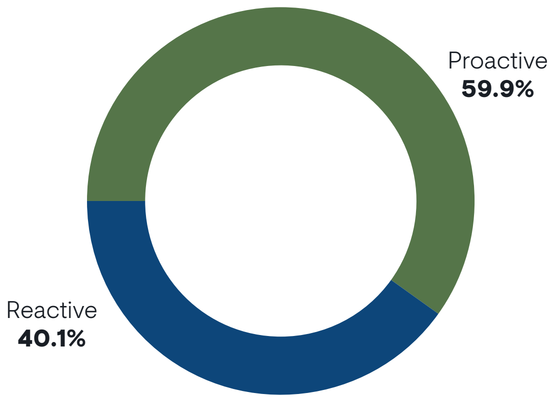
## Analysis:

Organizations were also asked how they allocated their resources on API security: more proactive (developing more secure APIs, testing and deployment of security solutions) or reactive (addressing breaches, security-related events, changing configurations based on attacks and threats). The respondents indicated that it was about a 60-40 split, with slightly more time being proactive.

## Commentary:

It was surprising that the responses were as evenly split as the responses indicated, since so many of the tools and solutions indicated require manual intervention (very few of the API security solutions have an automated threat component or an AI-based automated configuration or policy generation). Many organizations claim to address API security in the preproduction stage, but security teams and development teams likely divide their time equally from day-to-day firefighting and new projects. Prioritizing API security development and configuration proactively is not always a luxury that companies have the resources to enjoy.

WHAT PERCENTAGE OF YOUR TIME IS SPLIT BETWEEN BEING PROACTIVE AND REACTIVE AROUND API SECURITY EFFORTS TODAY?



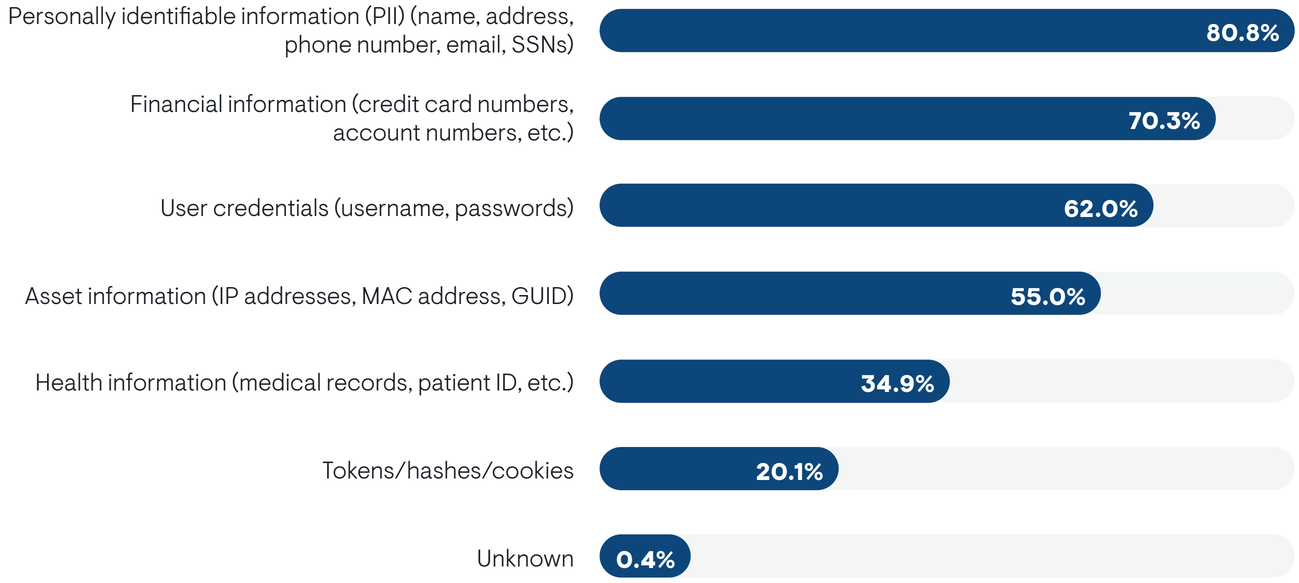
## Analysis:

Very little surprise from the first chart here: most APIs are used to share some sort of sensitive information, with personally identifiable information (PII) shared the most. Of greater concern is that respondents did not have visibility into the information being processed by applications and sent over their APIs. In this survey, over 25% felt that they had no visibility (to some degree) on the applications processing sensitive information.

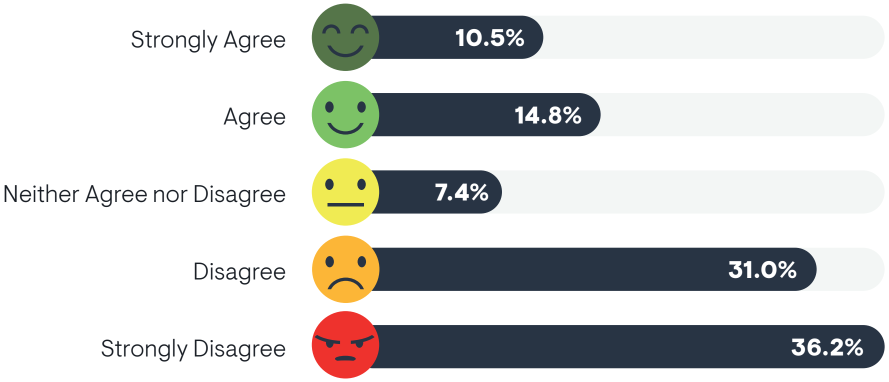
## Commentary:

To start, these graphs may be misleading. The respondent may not have direct insight into the information being processed by the applications, which could lead to a response of lack of visibility. Coupled with other questions from the survey, we find that this is actually a shockingly honest answer to an awkward question: many organizations do not have the visibility that they should have to safeguard the information that their APIs are transmitting and their applications are processing. Even in the most regulated industries that were surveyed, where you would expect this number to be 100% visibility, there were still significant respondents (over 5% depending on vertical) that lacked the necessary visibility and insights into the data being processed.

WHAT KIND OF SENSITIVE DATA DO THESE APIS PROCESS?



PLEASE RATE THE FOLLOWING STATEMENT:
I HAVE NO VISIBILITY ON WHICH APPLICATIONS ARE PROCESSING SENSITIVE INFORMATION.



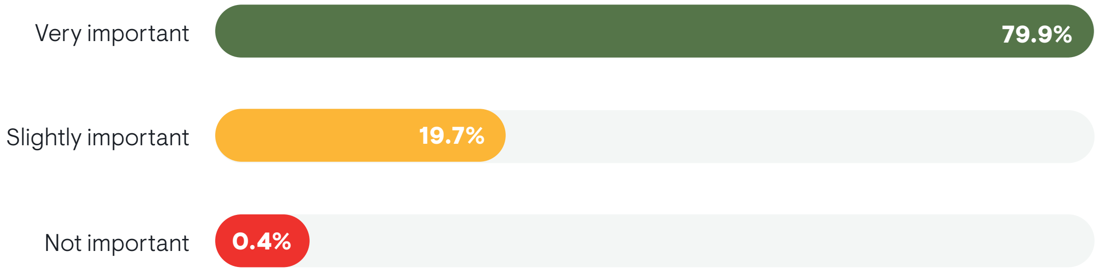
## Analysis:

Throughout this survey, questions were asked about how various tools and functions were integrated as part of the organization's overall API security strategy. In the case of threat hunting, nearly 80% of those surveyed responded that it was a very important part of their API security strategy.

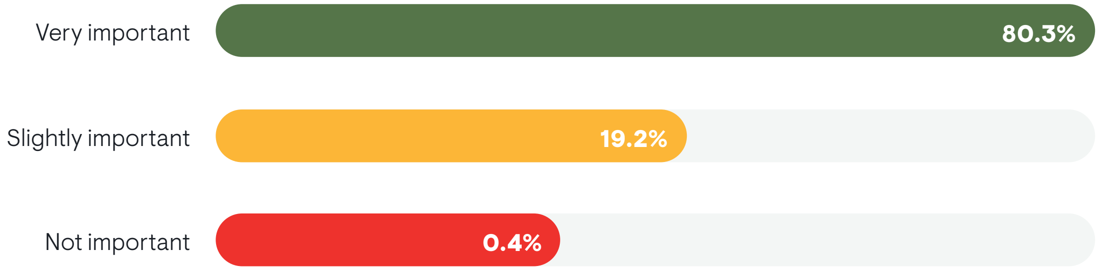
## Commentary:

Most of the tools used for API management have some basic sorts of security function, but few have a threat hunting capability. From a vendor perspective, it is important to build a threat hunting solution within your API management/security suite. For the customers of these solutions, it is important to find a solution that has native threat hunting capabilities or a strong integration with a threat hunting solution.

### HOW IMPORTANT IS THE ABILITY TO PERFORM THREAT HUNTING IN THE API ACTIVITY DATA?



### HOW IMPORTANT IS BEING ABLE TO INVESTIGATE AND UNDERSTAND THE ATTACK BY SEEING THE CONTEXT AND HISTORICAL DATA?



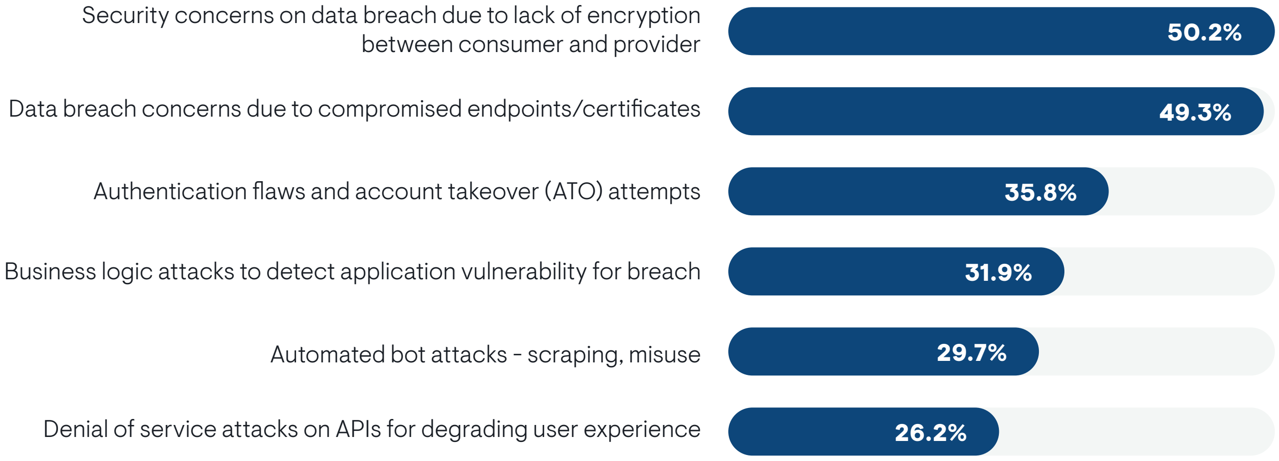
## Analysis:

Organizations are using a variety of solutions to detect threats to their APIs. API gateways was the most common choice (41%), with web application firewalls (WAF) and extended detection and response (XDR) solutions at the top. Data breaches and encryption challenges between connections appear to be the most common threats that organizations realized in the past 12 month. Almost 5% indicated that they didn't identify or didn't experience any attacks in their environments.

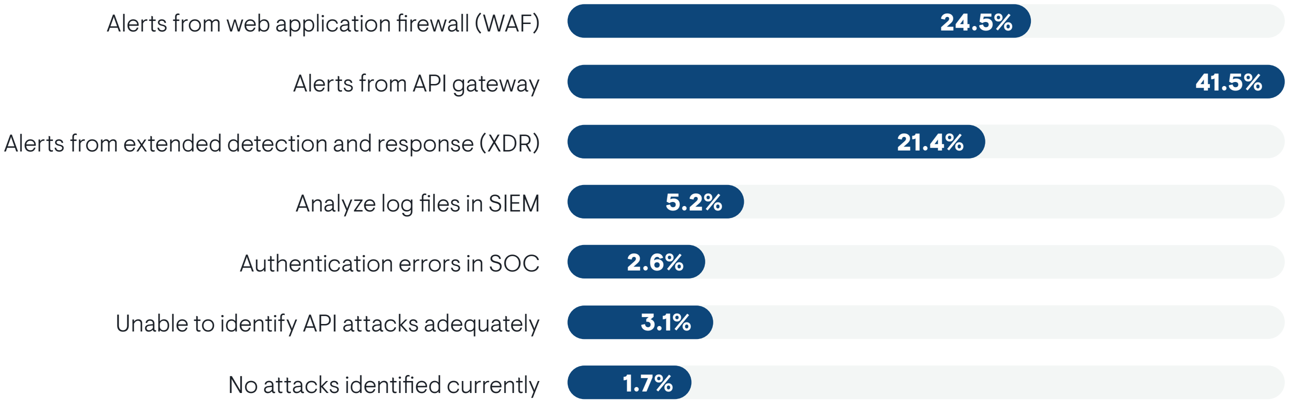
## Commentary:

When properly configured, API gateways, WAF, and XDR solutions can be used to detect (and in some cases respond) to attacks on APIs. The details are found in the configurations: solutions like API gateways, WAFs, and XDR are only as good as how they are configured. Plus, many APIs are either undocumented or unknown, making them nearly impossible to protect. Organizations deploy these API security tools with the belief that once they are deployed, they are magically secure, and no other efforts or solutions are necessary. No vendor would ever suggest this: they understand that they need to be constantly updated, monitored, and administered. Security—especially API security—is a constantly evolving threat landscape that requires constant revision and updates, something that most tools don't include as part of their offering.

WHAT ARE THE MOST COMMON THREATS YOU'VE SEEN ON YOUR APIS IN THE LAST 12 MONTHS?



WHAT IS THE PRIMARY METHOD YOUR ORGANIZATION CURRENTLY USES TO IDENTIFY AN ATTACK ON YOUR APIS?



# EMA Perspective

Most research reports are straightforward to craft: the results speak for themselves, whether it is the latest security solution or the direction that a specific market segment is trending. Not so with this report. While hoping to gain insights into how organizations are securing the APIs in their environment (and we did get some of that), the tone of the report shifted because the data shouts that most organizations have a false sense of how their APIs are secured and the efficiency of the tools they deployed to secure them. In fact, it could be even more basic than that, since many organizations believe that they have the personnel—API experts—that they need to adequately protect their APIs regardless of the solutions they have deployed.

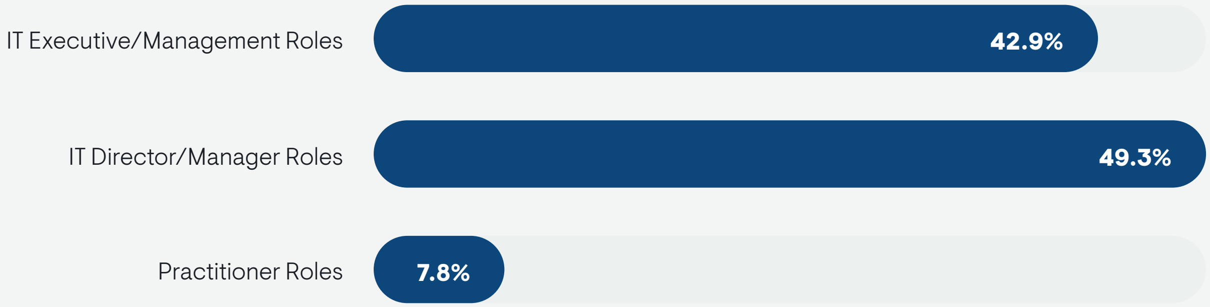
After reviewing the data, there are several takeaways that stand out and are worthy to be shared.

- Management understands the importance of API security. Over half of the organization surveyed indicated that their management grasps the need for API security. This is a strong indicator that management supports their DevOps and SecOps teams in purchasing and deploying API security solutions. Unfortunately, after the initial API security rollout and push occurs—the time that the executive decision-makers feel they have mitigated a potential risk—is also when the most concerning failures begin, since these executives are left with a false sense of security that a process for securing APIs is developed and implemented. Ninety-five percent believe their existing security tools are effective at protecting their APIs and believe that the solution purchased will safeguard their organization. They feel they have done all the right things, but a deeper look at the environment shows that there are still significant gaps that need to me remediated.
- One-quarter of all APIs are undiscovered or undocumented. On average, the fact that over ¼ of an organization's APIs are undocumented is the strongest evidence that organizations believe they have a "mature" API security strategy, but have subscribed to a false narrative. Certainly, there are tools that can help discover and document an organization's APIs, but this is also a process gap that needs to be reassessed by every organization, including those with strong API security procedures.
- API security should not wait until production. Thirty-two percent of those surveyed implemented API security standards in their production environment. This is often far too late to have a real impact, since API controls and procedures should be implemented at the time of design and development. Simply put, the opportunity to miss a step or control once deployed into production is part of nearly all security failures and will certainly be so regarding API security.
- Integrations are key. For those that have a baseline understanding of their API environment, using existing API security and management tools to integrate with other security solutions is critical. Threat hunting and detection is certainly one of many security solutions that is essential to having a complete picture on how best to deal with API security. Customers would be wise to have a broader understanding of how their existing API management tools integrate with their overall security solutions and seek vendors that provide guidance on how to maximize their integrations.

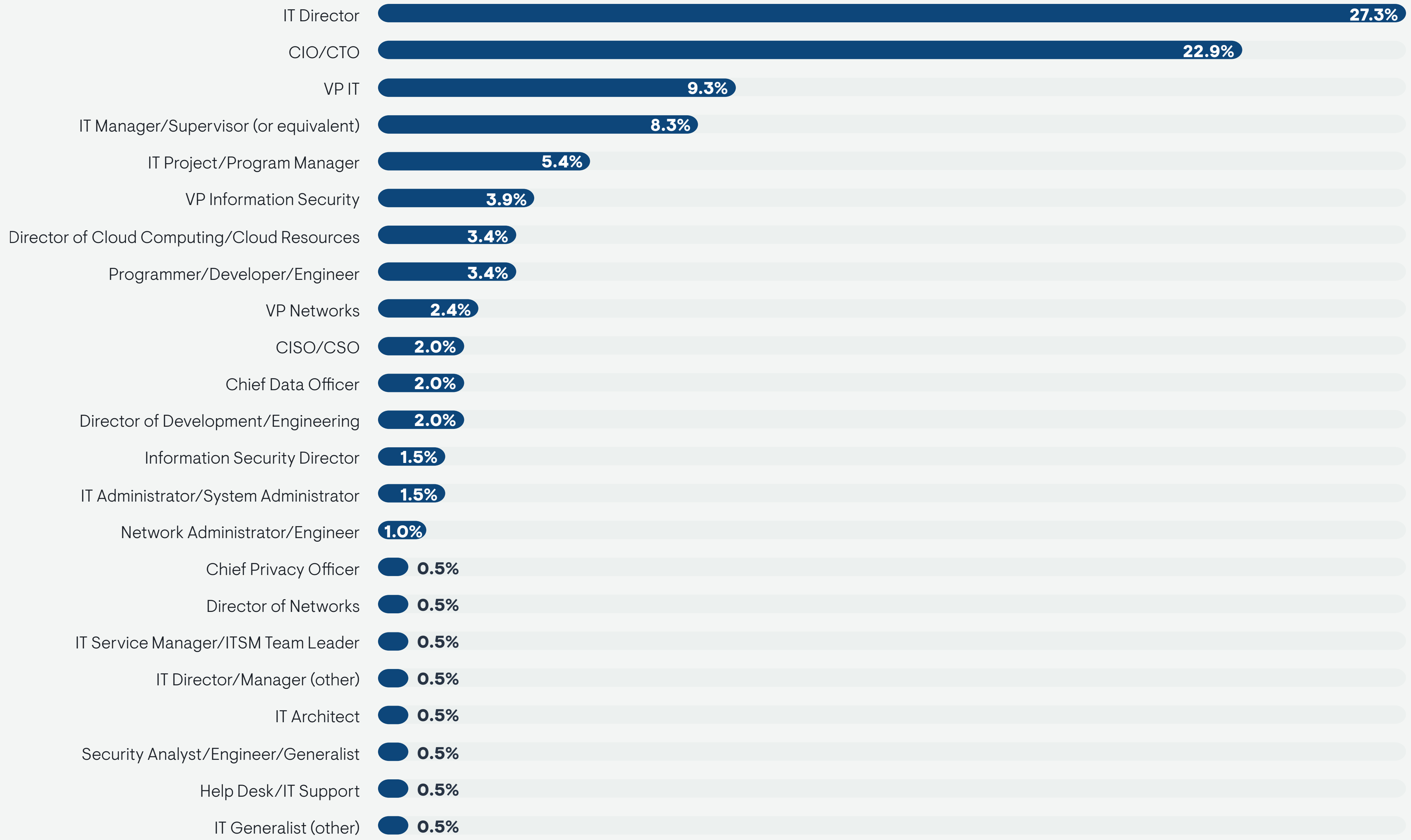
Even talking about API security is a significant shift from previous years. Anecdotally, the researcher had a discussion with a particular client in the financial services space that shared that one of their high-traffic APIs had been in place for over 18 years without significant modification, due to SLAs and the inability to prioritize changes/updates to their environment. No company or organization wants to be insecure, and by shedding light on the significant security gaps most organizations have with their API infrastructure, the security industry can make incremental steps to improving these challenges.

# Research Methodologies and Demographics

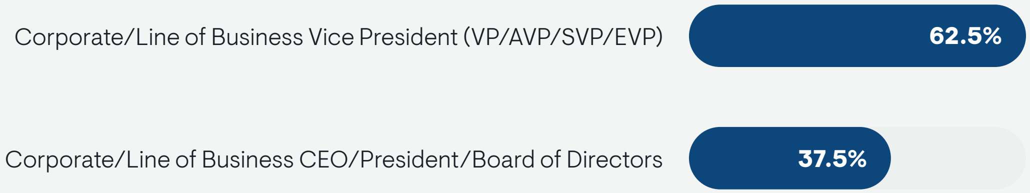
## YOU INDICATED THAT YOUR DEPARTMENT IS IT-RELATED. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR SPECIFIC ROLE?



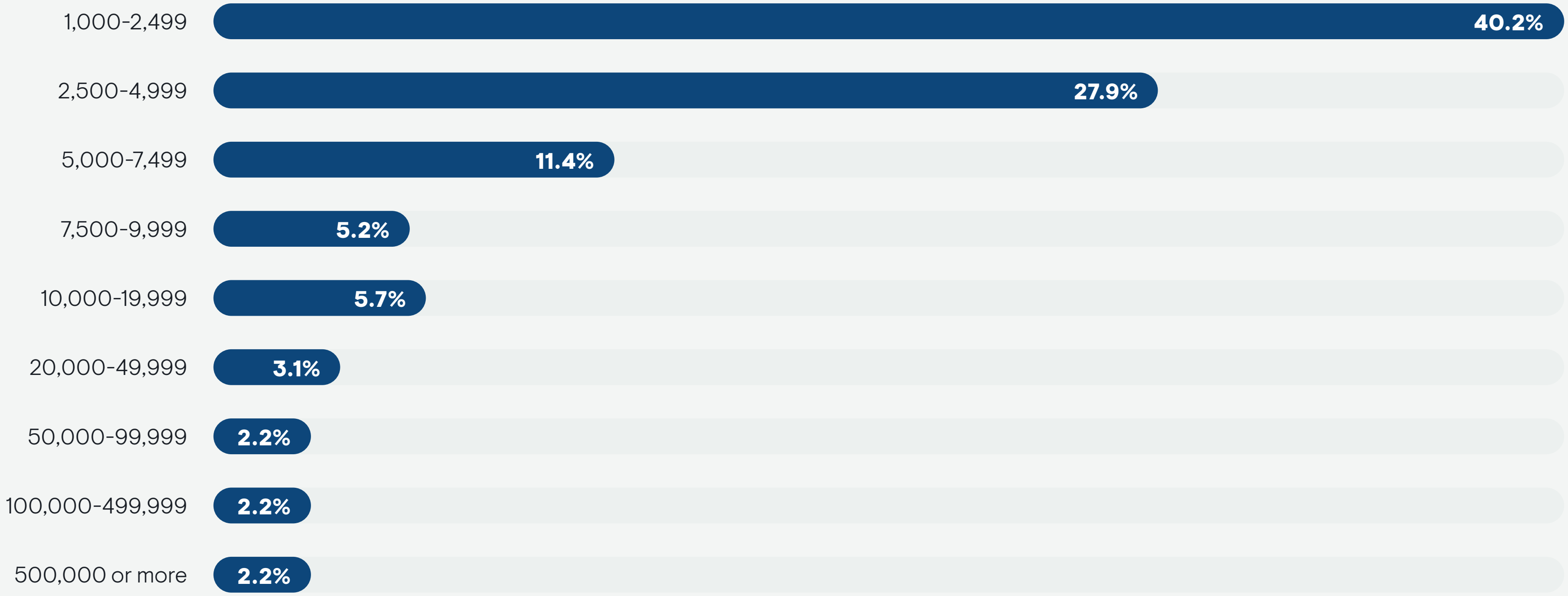
## YOU INDICATED THAT YOUR DEPARTMENT IS IT-RELATED. WHICH OF THE FOLLOWING BEST DESCRIBES YOUR SPECIFIC ROLE?



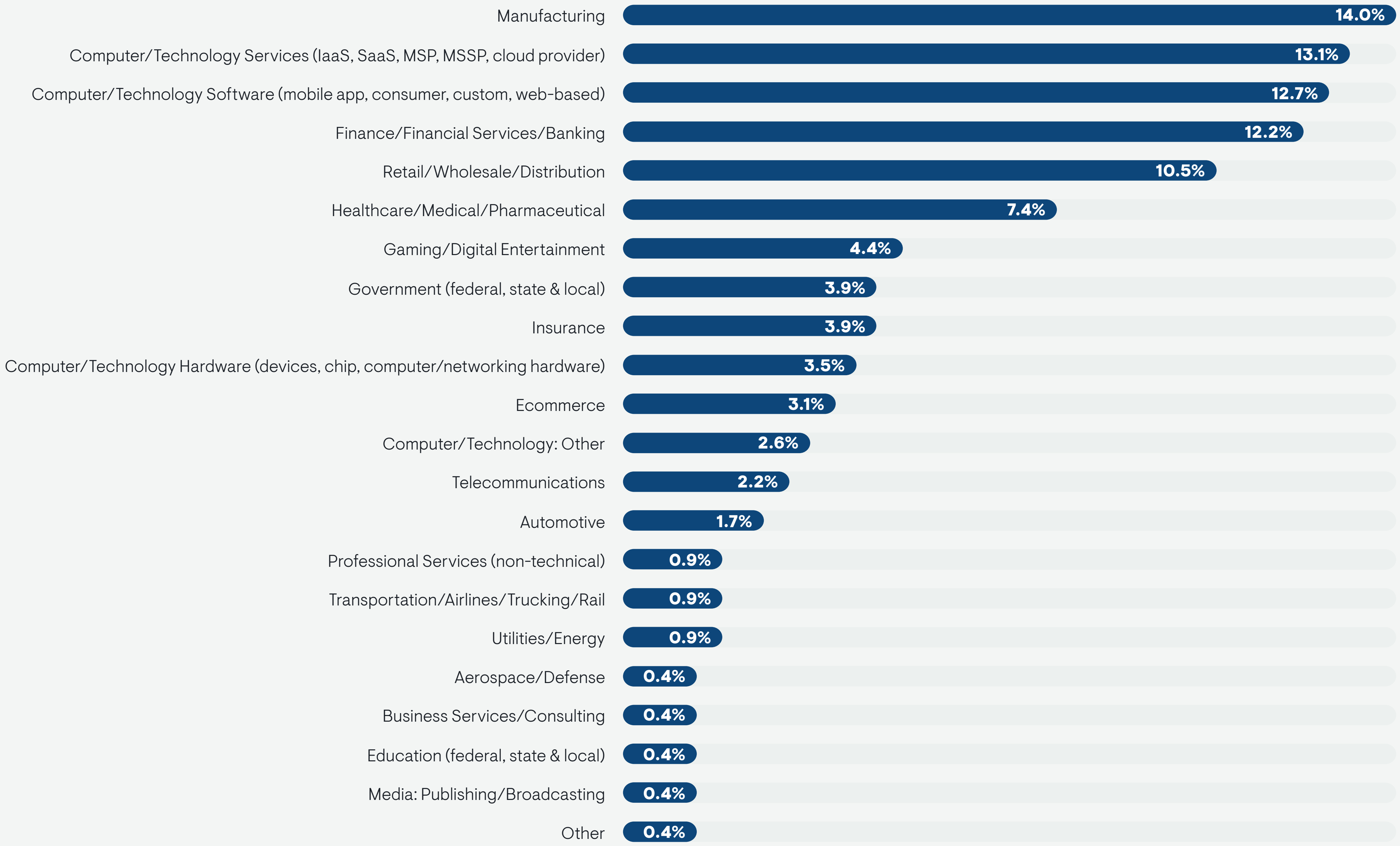
## WHICH OF THE FOLLOWING BEST DESCRIBES YOUR SPECIFIC ROLE IN YOUR ORGANIZATION?



## IN TOTAL, HOW MANY EMPLOYEES ARE CURRENTLY WORKING IN YOUR ORGANIZATION?



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.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com 4255.082523