451 Research
Vanguard Report
April 2024

Digital transformations rely on APIs — and ineffective API security can open the door for attackers

Commissioned by
graylog

S&P Global
Market Intelligence

Introduction

Digital transformation (DX) projects remain a priority for organizations even in the face of economic headwinds. Primary DX drivers include improving workforce productivity and engagement, improving customer experience and reducing costs through operational efficiencies, according to 451 Research's Voice of the Enterprise (VotE): Workforce Productivity & Collaboration, Digital Transformation 2023 survey. The study results indicate that organizations will continue allocating a significant portion of IT budgets to these initiatives over the next two years.

DX projects also face barriers including the complexity of legacy applications, overcoming organizational hurdles and silos, embracing business process change management and potential failure to secure sensitive data. At the same time, the move to cloud continues unabated, with future software investments primarily driven by cloud deployments and technologies that ease integrations with existing enterprise software. DX, combined with the increasing pace of cloud adoption, has led to an increasing prevalence of and dependence on application programming interfaces (APIs) — the "services glue" that enables interoperation of these systems. Attackers, realizing this, have increasingly focused on exploiting APIs, which can provide access to a wealth of sensitive and valuable data and systems even while their exploitation is notoriously difficult to detect. This paper focuses on API security, including key capabilities, trends and potential solutions.

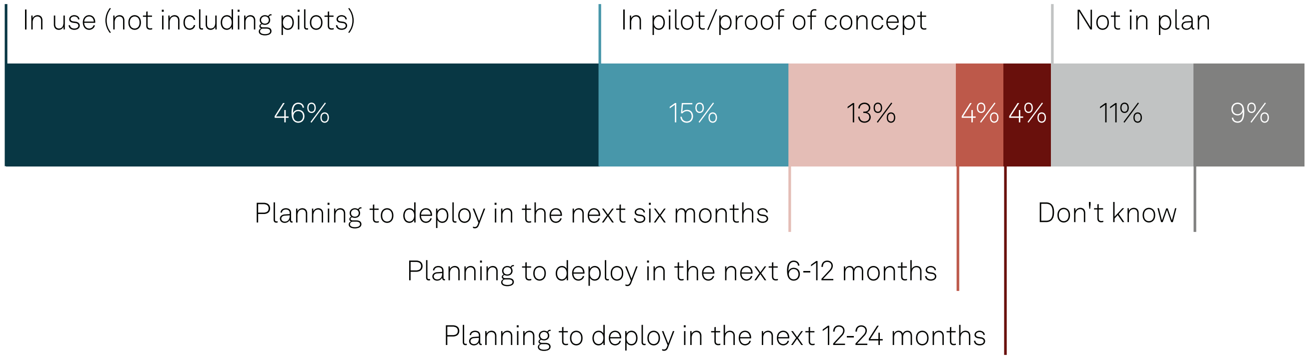
The Take

Since APIs operate silently in the background, they can be difficult to secure. API security requires controls that ensure data confidentiality, integrity and availability — including authentication and authorization, encryption, monitoring/logging of API activity, and scanning for and remediating API vulnerabilities. Because APIs are being added every day, organizations need a way to inventory and discover new APIs being used in corporate networks. From an operational perspective, API security often falls into a coverage gap between security and DevOps, with assumptions being made that secure coding practices, a solid QA program and an API gateway provide adequate protection against attacks. Unfortunately, an API can be coded securely, operate as intended, display great performance, and still be a data exfiltration path, so an additional layer of runtime production monitoring is required.

Failure to properly secure APIs can expose endpoints, enabling attackers to assume user identities, manipulate back-end systems, create denial-of-service (DoS) incidents, increase operational costs and enable "man in the middle" attacks, to name but a few possible consequences. Monitoring APIs can be difficult because they are used everywhere — in on-premises systems, cloud applications, IoT/OT and mobile devices. And once they leave the application server, encryption makes them even more difficult to discover and monitor.

API security is clearly a key pain point for organizations. In 451 Research's VotE: Information Security, Technology Roadmap 2023 study, 46% of respondents indicated they are using API security (up 14 percentage points over 2022 data), and another 15% are in pilot/proof of concept, totaling 60% that are using it or are in the deployment process. An additional 20% of respondents are planning to deploy in the next 24 months, leaving only a little over 19% that have no plans or did not know their organization's plan. API security spending is also keeping pace, with 34% of respondents planning significant increases in spending and 41% planning slight increases over the following 12 months, so nearly three-quarters of respondents are increasing spending to some degree. While this indicates a significant upward trend in API security adoption, selecting the correct solution may be eluding some organizations, a potential reason for continuing increases in spending despite the high adoption rate. The spending increases may also be due to extending current API security deployments after an initial rollout.

Figure 1: API security implementation status



Q. What is your organization's status of implementation for the following information security technologies? API security.
Base: Respondents whose organizations have at least one information security technology in use (n=164).
Source: 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2023.

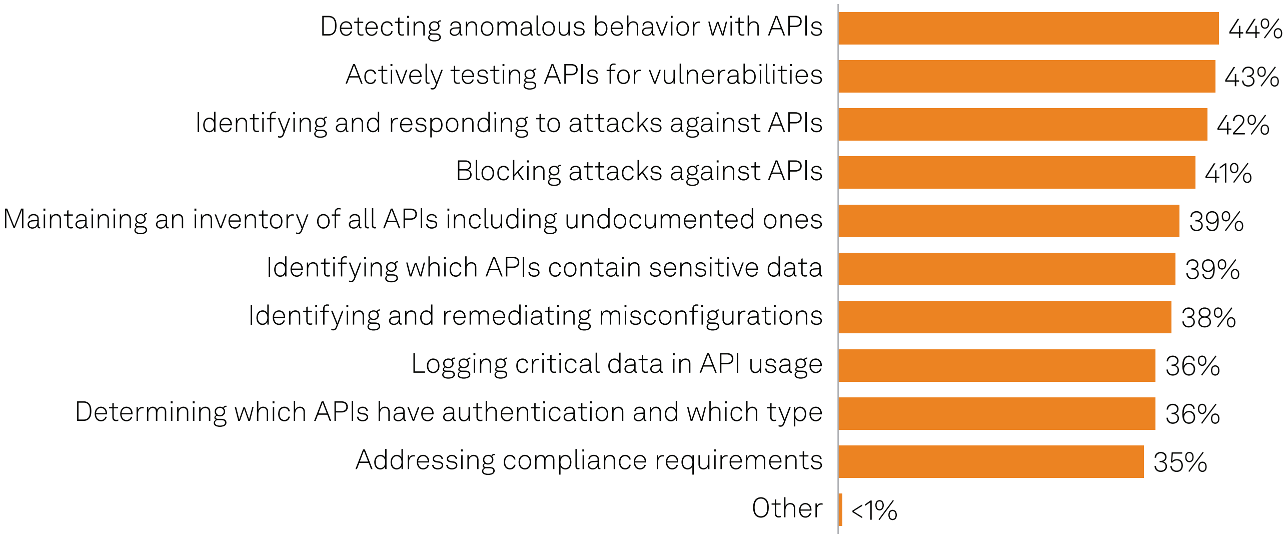
Traditional approaches to API security included perimeter protection through web application firewalls and API gateways, plus classic vulnerability-scanning techniques. While these approaches provide some protection, they leave gaps in coverage:

- Perimeter defenses may not stop attackers from using stolen identities.
- Detecting new APIs and inventorying existing APIs in use can be difficult due to encryption.
- Solutions that rely on API header analyses don't provide a full picture of API activity, which requires the ability to examine the entire API payload to support threat analysis, threat hunting and forensics use cases.
- Many API security solutions are designed for cloud or on-premises — but not both — and may lack support for multiple cloud providers and hybrid architectures.
- Other API security solutions do not account for privacy and compliance issues such as filtering, redaction and anonymization that are required by regulations such as General Data Protection Regulation (GDPR) and internal policies. Another consideration is where sensitive API data is processed because data sovereignty can be a major compliance issue.
- Many successful API attacks are multistage and involve requests that may appear to be legitimate, bypassing signature-based identification approaches.

Use cases

451 Research's Voice of the Enterprise: Information Security, Application Security 2023 asked more than 900 senior IT professionals to rank their top API security tool requirements (see Figure 2). The top seven responses are detecting anomalous behavior with APIs (44%), actively testing APIs for vulnerabilities (43%), identifying and responding to attacks against APIs (42%), blocking attacks against APIs (41%), maintaining an inventory of APIs including undocumented ones (39%), identifying which APIs contain sensitive data (39%), and identifying and remediating misconfigurations (38%). Other important features include logging critical data in API usage (36%), determining which APIs have authentication and the type of authentication used (36%), and addressing compliance requirements (35%).

Figure 2: The most important features of an API security tool



Q. What are the most important features of an API security tool? Please select all that apply.
Base: Respondents currently using application security or plan to over the next 12 months, abbreviated fielding (n=220), top seven responses.
Source: 451 Research's Voice of the Enterprise: Information Security, Application Security 2023.

Detecting anomalous API behavior

OWASP, a non-profit organization, publishes an openly accessible "API Security Top 10" list of API weaknesses that provides a good starting point for understanding common ways that APIs can be exploited. And while this is far from a definitive list of all weaknesses, one approach to detecting anomalous behavior is just that — understanding an API's intended purpose and monitoring for anomalous behavior. This can include detecting unusual authentication activity such as using abnormal credentials, using the API to access data or systems that it does not usually access, identifying an API that is causing unusually high resource usage, and so on. These tactics can be particularly useful in detecting zero-day or novel attacks that have not been discovered and publicized. And while most modern security analytics platforms are capable of detecting these activities by correlating signals from multiple sources and applying anomaly detections through behavioral analytics, they must first have a way to acquire those signals. The depth of the telemetry provided is also key — being able to perform deep inspection inside of the API payload enables a richer set of analyses.

Actively test APIs for vulnerabilities

Scanning APIs and the systems that rely on them for vulnerabilities can be performed with classic vulnerability management tools; however, many do not perform deep API analytics such as traffic inspection. A specialized API vulnerability scanner can provide higher-quality scans, as well as detect potential vulnerabilities in undocumented APIs that traditional scanners might miss.

Identify and respond to attacks against APIs

Peter Drucker is often credited with the statement, "You can't manage what you can't measure." Effectively detecting and responding to API attacks can be enhanced with specialized technology that can acquire the necessary detection signals and can also correlate signals with API-specific tactics, techniques and procedures (TTPs) such as those published in the MITRE ATT&CK knowledge base. This not only assists in API attack detection but can also improve remediation time since it can provide an understanding of the complete attack chain. The same set of signals and TTPs can be applied to other systems in the environment, helping to ensure that other systems using the same API do not fall victim as well.

Block attacks against APIs

Once an organization has acquired an understanding of the overall API attack surface, blocking current and potential API attacks is a critical next step. This can include resolving API vulnerabilities, employing proactive blocking techniques such as tuning firewall rules to help prevent unauthorized access to APIs and detecting API weaknesses such as a lack of encryption. Before this can occur, a process must exist to collect the data that network and security administrators require to build these defenses, including an exhaustive list of known APIs and their normal behavioral patterns.

Maintain an inventory of APIs, including those that are undocumented

Gaining an understanding of which APIs are in use by an organization can be a difficult task, particularly when all environments are considered, including on-premises, private clouds, multiple public clouds and hybrid environments. The output of this inventory should include a list of previously undetected APIs that need to be investigated, and the API security technology must be capable of enabling these activities. This includes determining how the APIs are used, whether they are being used by legitimate business systems, and which identities are being used to access the API, as well as adding newly discovered APIs to a database and notifying security staff of suspicious API activity.

Identify which APIs contain sensitive data

Identification of APIs that contain sensitive data is a key compliance requirement. Privacy has become a major regulatory issue over the past decade, with privacy laws such as the EU's GDPR and the California Consumer Privacy Act (CCPA) — in addition to longer-standing regulations such as the US Health Insurance Portability and Accountability Act (HIPAA) — requiring organizations to maintain a complete understanding of how their users' personal data is collected, processed and stored. Fortunately, many of the same technologies used for compliance mandates can also be used to manage and secure sensitive organizational data. Once again, a key requirement is the ability to see inside of API calls to detect potential sensitive data, offering a richer set of sensitive data detection capabilities.

Identifying and remediating misconfigurations

Misconfigurations are a leading cause of data breaches, and APIs are no exception. The ability to detect a misconfigured API — or applications that are misusing the API — is a high priority for security organizations. To effectively identify misconfigurations, an API security tool must be capable of testing API calls and monitoring their usage in real time. Providing a full set of API misconfiguration data to operations and development personnel is also key to ensuring effective remediation.

Conclusion

APIs are a key enabling technology used to deliver today's hyperscale, rapidly digitally transforming business environments. Application integration requirements, which can exist inside of traditional organizational perimeters as well as in one or many cloud environments, are growing faster than ever, and many in use are undocumented or "shadow" APIs. Application developers and vendors commonly create new or extend existing APIs to support technical requirements, without necessarily taking security into account. In other cases, APIs designed for internal use only may be used to integrate with a third-party application, outside of the firewall. This has resulted in demand for the ability to effectively detect, inventory, monitor, control and scan APIs for security weaknesses and illicit use.

Traditional API security approaches that rely on perimeter protection and analyze header information may not provide the level of protection required to effectively manage today's threat landscape. Consider investing in deeper inspection techniques that enable security analysts to see inside of API calls, from the inside, before encryption makes the task very difficult — providing required API detection, monitoring and control capabilities.

About the author

Mark Ehr

Principal Research Analyst, Security

Mark is a principal research analyst on the 451 Research cybersecurity research team of S&P Global Market Intelligence. He focuses on cybersecurity with an emphasis on cloud security, security operations and AI/ML. Mark has more than 20 years of cybersecurity experience plus a decade in software development and many years in computer networking. In his time at S&P, Mark has delivered go-to-market projects and contributed to S&P's 451 Research team in areas including SIEM, secure access service edge (SASE), network security, private key infrastructures (PKIs), AI, continuous security validation and threat modeling.

Before joining S&P Global in 2022, Mark spent 12.5 years at IBM, including three years in BigFix endpoint management product marketing, four years as a QRadar SIEM product manager, and six years leading security sales enablement across IBM's $1 billion threat management product family. He also spent four years as an industry analyst at Enterprise Management Associates.

Mark holds a bachelor's degree in computer science from Metropolitan State University of Denver with an emphasis on electronics engineering technology and is an ISC^2 Certified Information Systems Security Professional (CISSP). He also jokes that he holds an "MBA from the school of entrepreneurial hard knocks," gained in his five years as an equity partner in a Boulder, Colorado-based software firm.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.