One-Minute Insight Report

2021 State of API Security, Privacy, and Governance

Data collected from July 22 - September 16, 2021
Respondents: 300 technology decision-makers

PULSE | CLOUDENTITY

2021 State of API Security, Privacy, and Governance

APIs (Application Program Interface) are the underpinnings of app modernization and digital transformation, connecting users and systems to a network of services, applications, and databases.They are a key component of web applications and cloud computing. As the fabric of modern service delivery and compartmentalized app development, the application logic and sensitive data APIs expose has made them a high-value target of threat actors. Progressing API security is paramount to ensure the integrity, management, and protection of those internal and external-facing API / service pathways.

As part of API First programs, developers and DevSecOps teams are endeavoring to modernize and better manage API inventory, access, data privacy and compliance controls - inclusive of authentication, authorization and privacy consent. This 2021 State of API Security, Privacy and Governance report shows how enterprises are advancing API First programs in their organization and reveals key drivers, adoption, technologies, initiatives, investments and benefits.

This 2021 State of API Security, Privacy and Governance report surveyed 300 technology decision-makers and practitioners that manage or are responsible for API management and security within enterprises of 10,000 employees or more across financial services, healthcare, hightech, retail, consumer goods and manufacturing industries. Highlight findings include:

Issues

At least 44% of respondents expressed substantial issues concerning privacy, data leakage, and object property exposure with internal or external-facing APIs.

Impact

72% of enterprises had moderate/significant delays in releases of new applications and service enhancements due to identity and authorization issues with APIs and services.

Cause

Component-driven development complexity, difficulty to diagnose issues and lack of data lineage, and inconsistent security policy management among the top 5 contributors to API identity and authorization risks.

Maturity

83% of organizations expressed that their API/service authorization policy management is decentralized with some policy standards and implemented by directly coding per application, with more than 62% aspiring to improve their API development and authorization governance programs.

Top Drivers

Critical drivers to initiate or augment secure API development and API security programs include reducing coding human error, preventing sensitive data leakage, ensuring compliance, and ensuring data privacy/privacy consent, and preventing threats.

Investment

93% plan to increase budget and resources applied to secure API development and security programs, and the majority (64%) plan an increase as much as 15%.

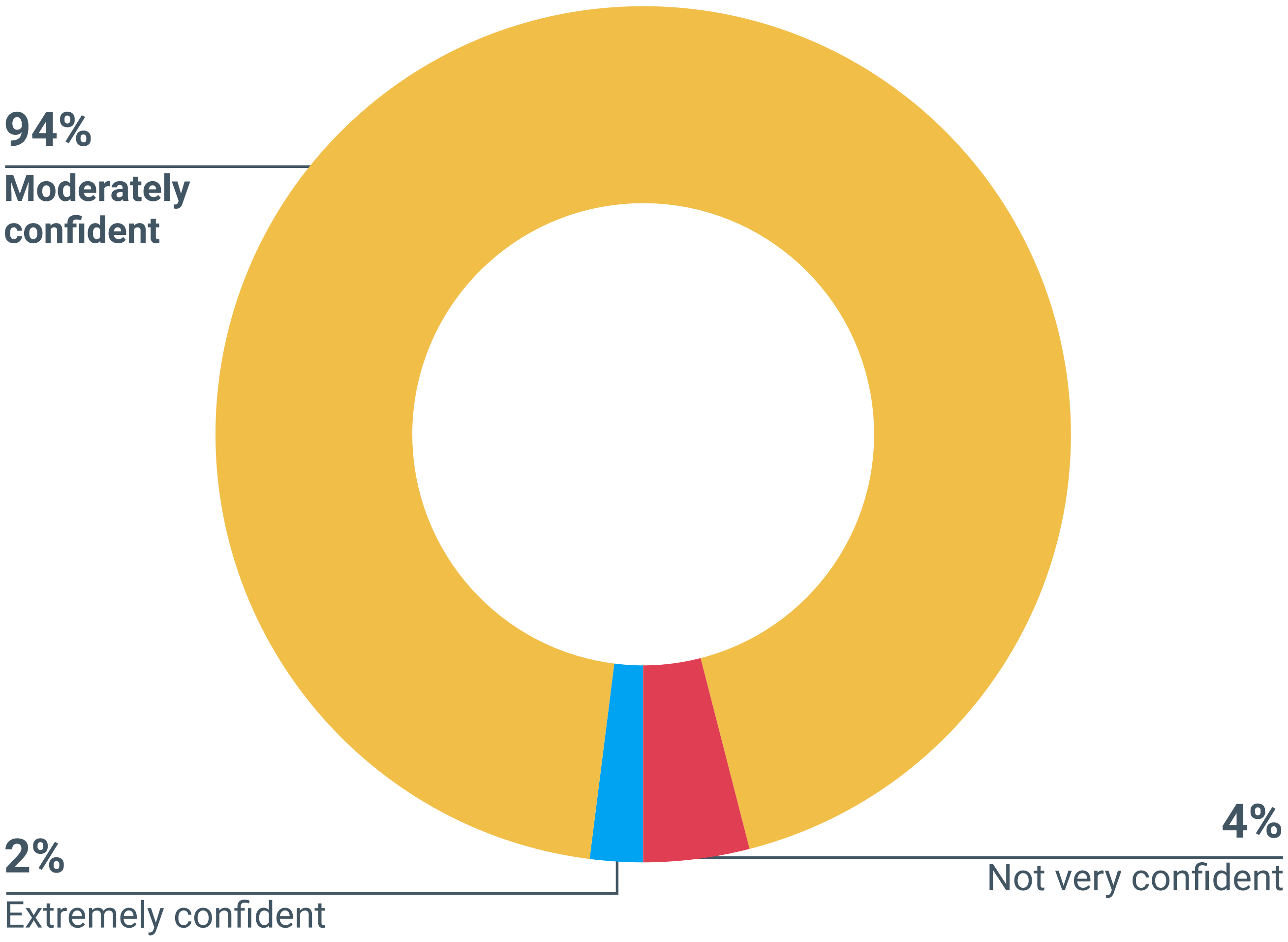
Initiatives

Top five API security initiatives include implementing Zero Trust controls, invoking declarative authorization (policy as code), enabling privacy consent management, and facilitating API intelligence.

Confidence

Almost all (94%) decision-makers are **only moderately** confident in their organization's ability to materially reduce API data security issues.

How confident are you in your organization's ability to materially reduce API data security issues such as unauthorized access, threat, data privacy and compliance risks?

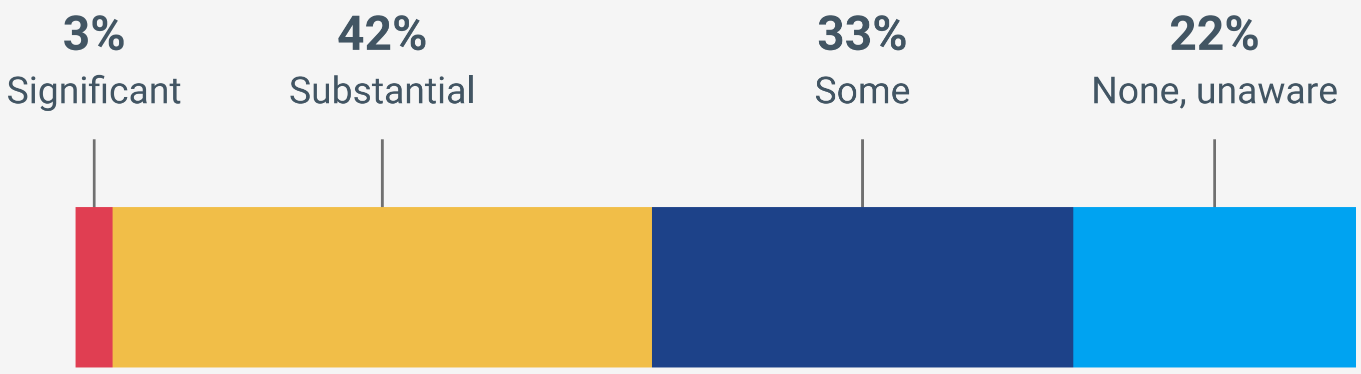


Issues

44% of respondents have experienced at least substantial API authorization issues **concerning privacy, data leakage, and object property exposure** with one or both of internal and external-facing APIs.

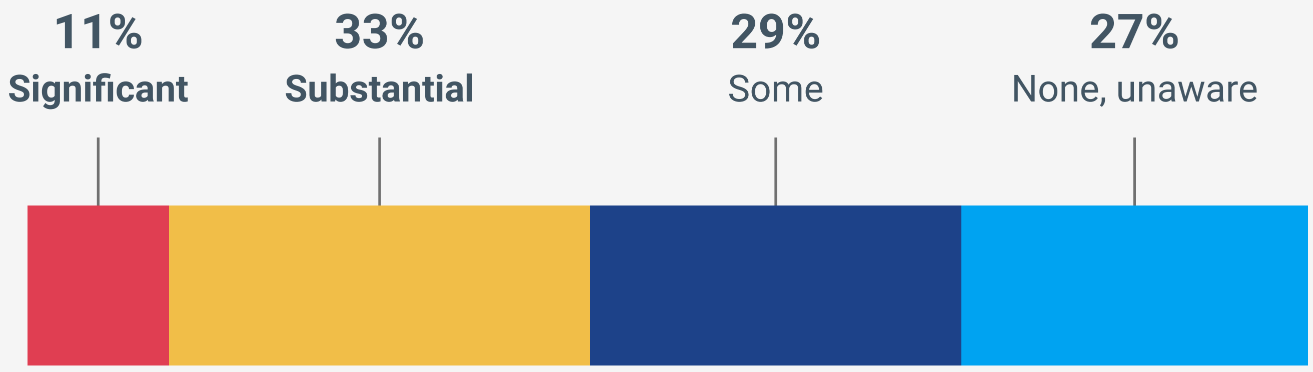
In terms of internal or partner-facing API authorization issues, a majority of respondents say they have had some or substantial issues.

In the past 12 months, to what degree has your organization experienced the INTERNAL / PARTNER-facing API authorization issues concerning privacy, data leakage, object property exposure?



Most respondents say they have also experienced some or substantial external or customer-facing API authorization issues in the past 12 months - **over a third expressing substantial issues**. This is also consistent amongst all regions, but may vary by industry.

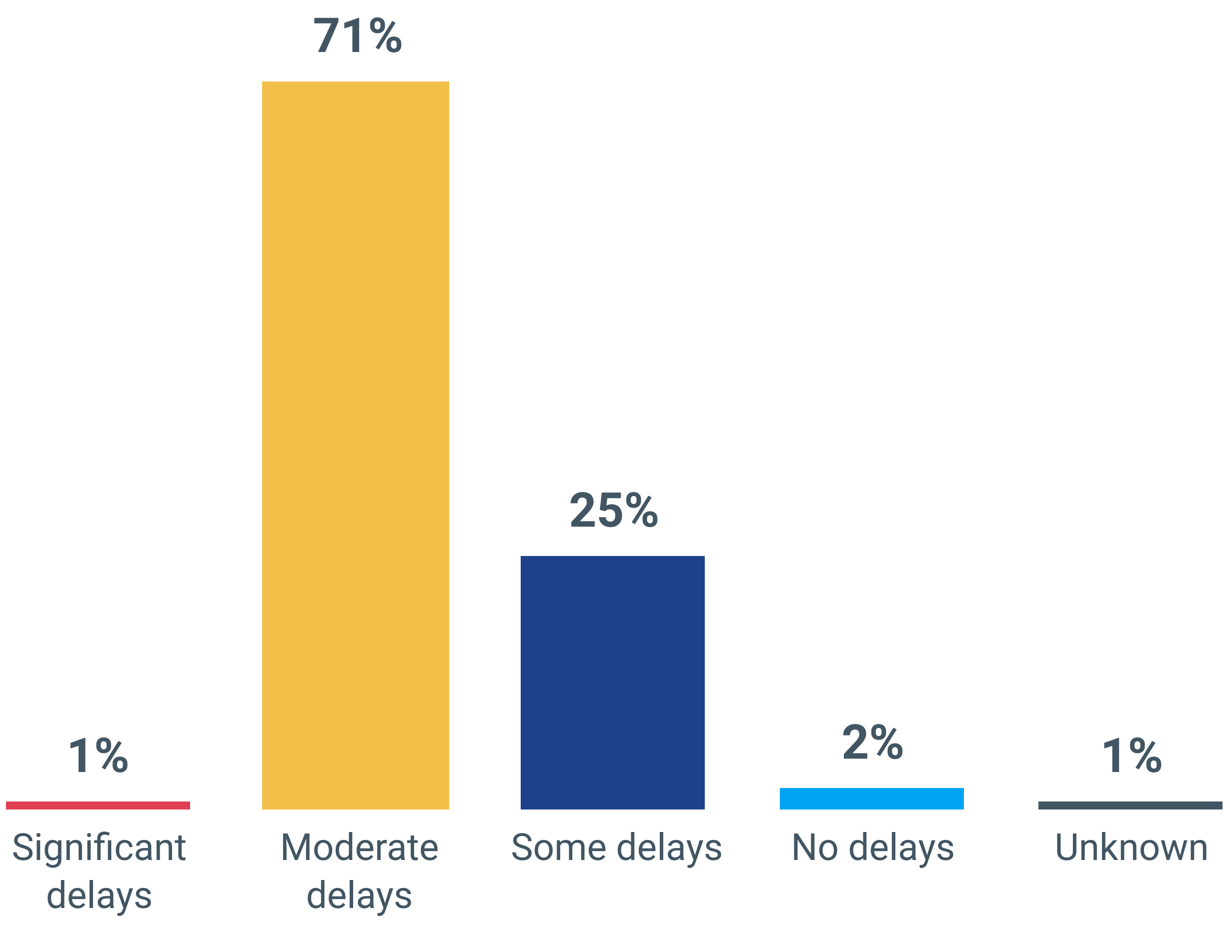
In the past 12 months, to what degree has your organization experienced the following EXTERNAL / CUSTOMER-facing API authorization issues concerning privacy, data leakage, object property exposure?



Impact

For 97% of respondents, identity and authorization issues with services and APIs have had a direct impact on their organizations in the form of delays to new application or service enhancements. **71% expressed visible delays** to releasing new application or service enhancements.

In the past 12 months, to what extent has new application or service enhancements been delayed due to Identity and Authorization issues with services / APIs?

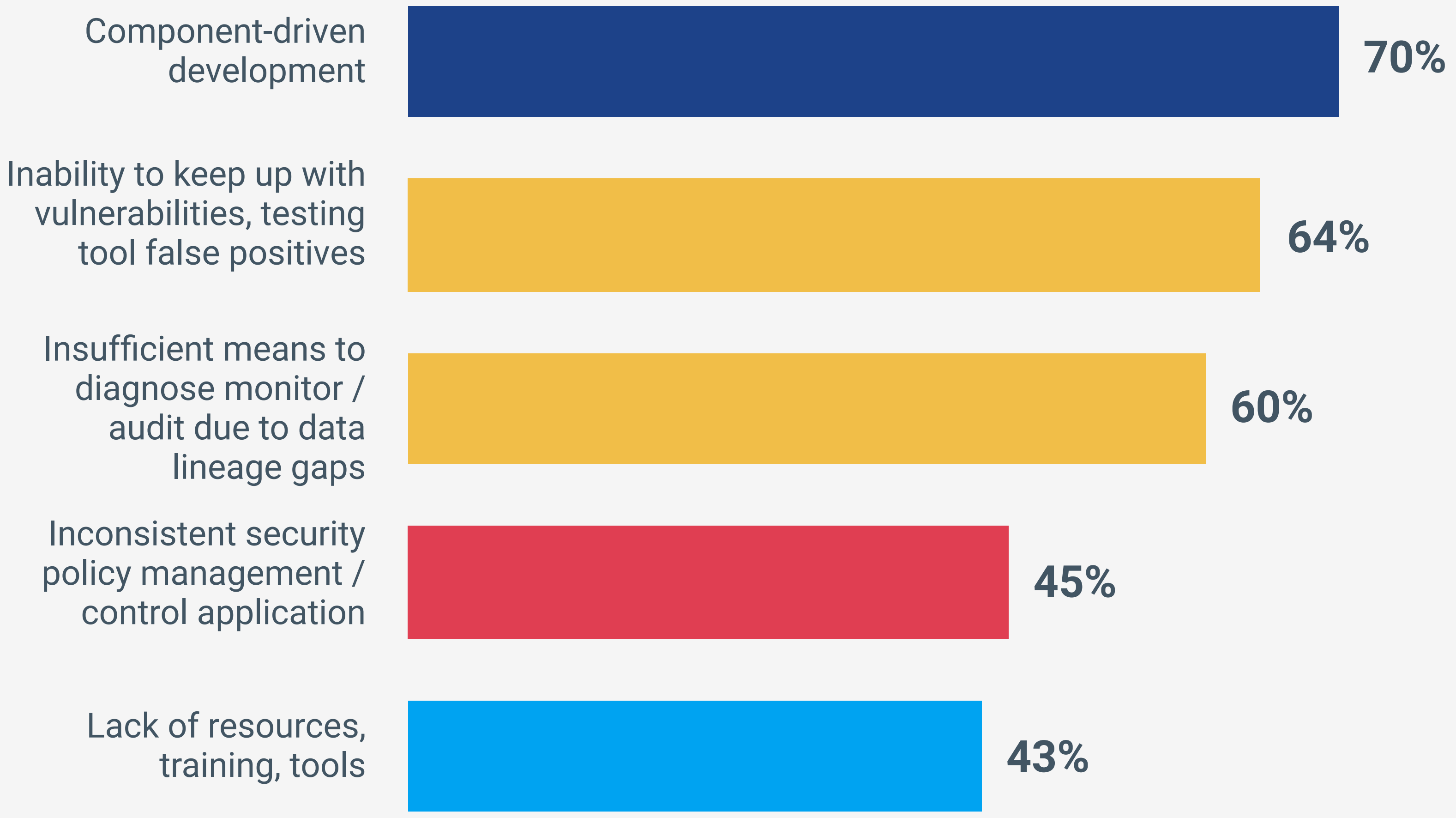


CLOUDENTITY

Cause

The top 5 contributors to API identity and authorization risks are component-driven development complexity, inability to keep up with vulnerabilities, insufficient means to diagnose and audit due to data lineage gaps, inconsistent security policy management / control application, and lack of resources, training, and tools.

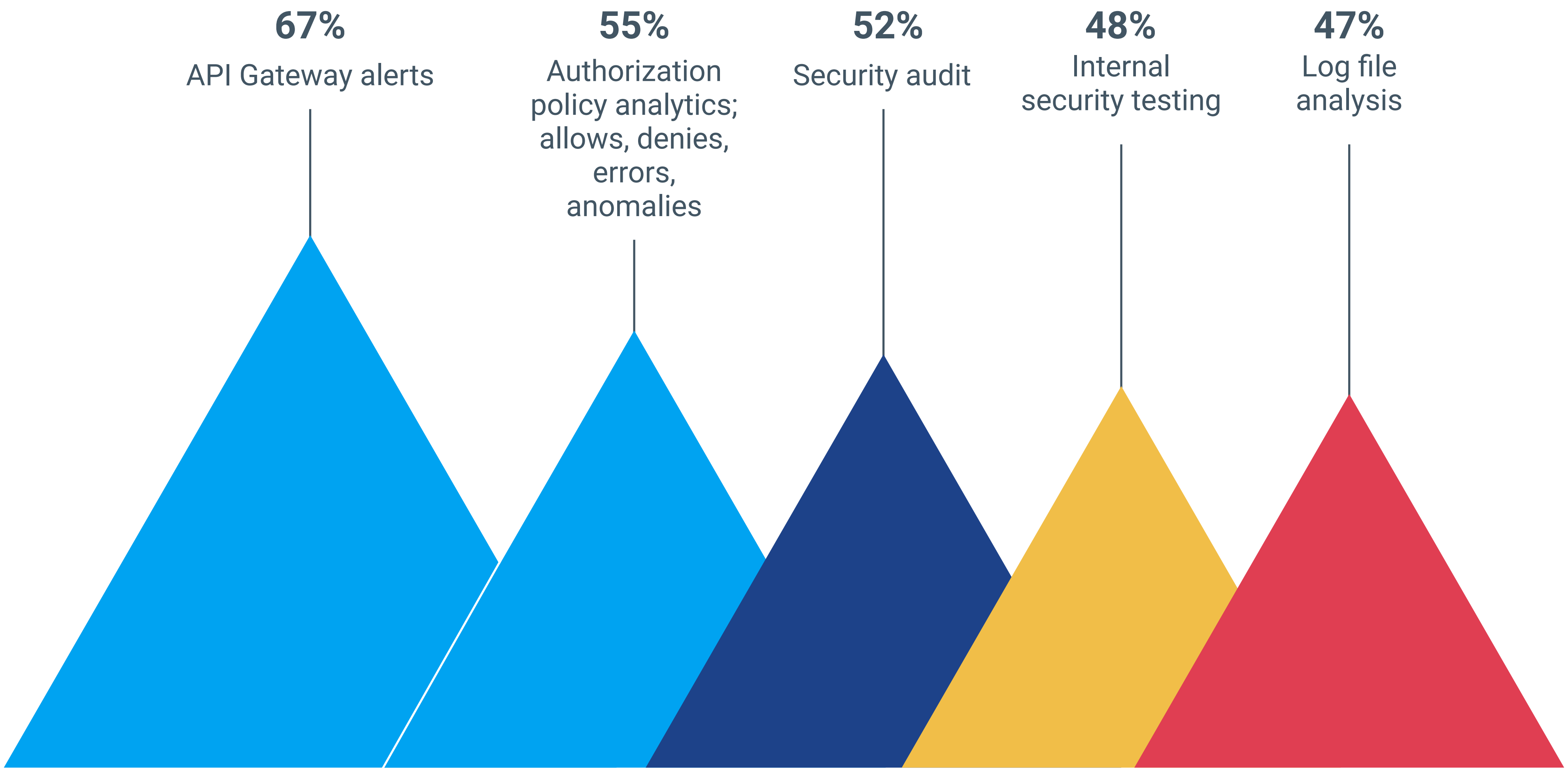
What do you feel is contributing to your organization’s API Identity and Authorization risks?



Mitigation

The most common mechanisms for mitigating API Identity and Authorization issues are API Gateway alerts, authorization policy analytics, security audits, internal security testing, and log file analysis.

What mechanisms are used to identify API Identity and Authorization issues in your organization?

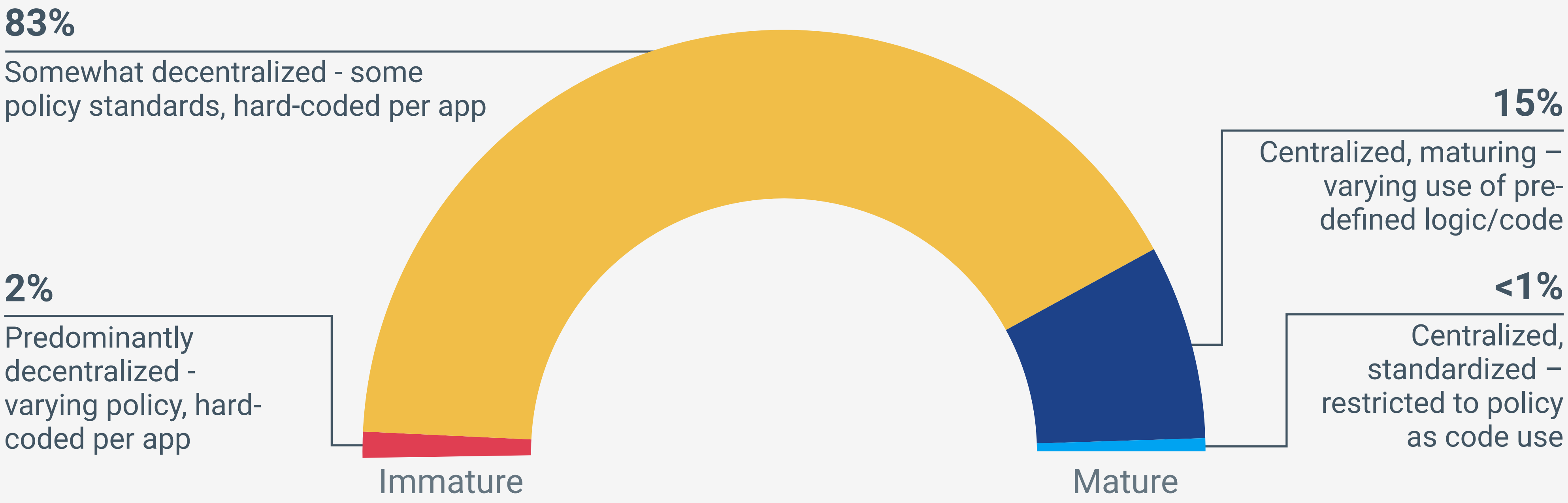


Maturity

85% of respondents report they have a mainly decentralized level of service or API authorization policy management in their organization - **which appears to indicate the majority will be progressing their relatively immature governance controls**. However, the level of service or API authorization policy management is comparatively more often centralized and maturing in healthcare (25%) and retail (27%) industries.

API Authorization and Privacy Governance Maturity

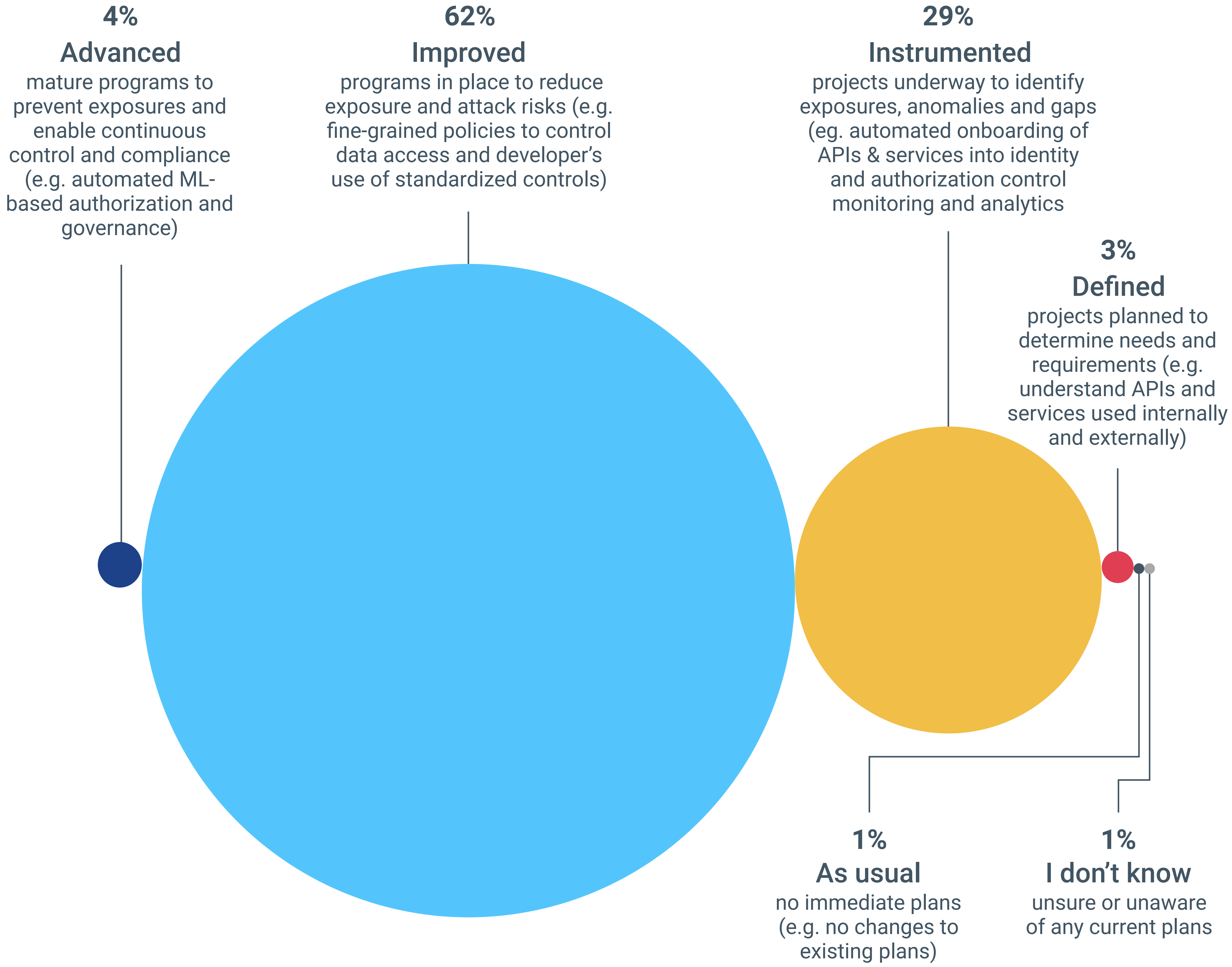
What is the level of service/API authorization policy management in your organization?



Aspirations

About two-thirds (66%) of decision-makers say they intend that their company's secure API development and authorization governance programs will become more improved or advanced over the next 12 months.

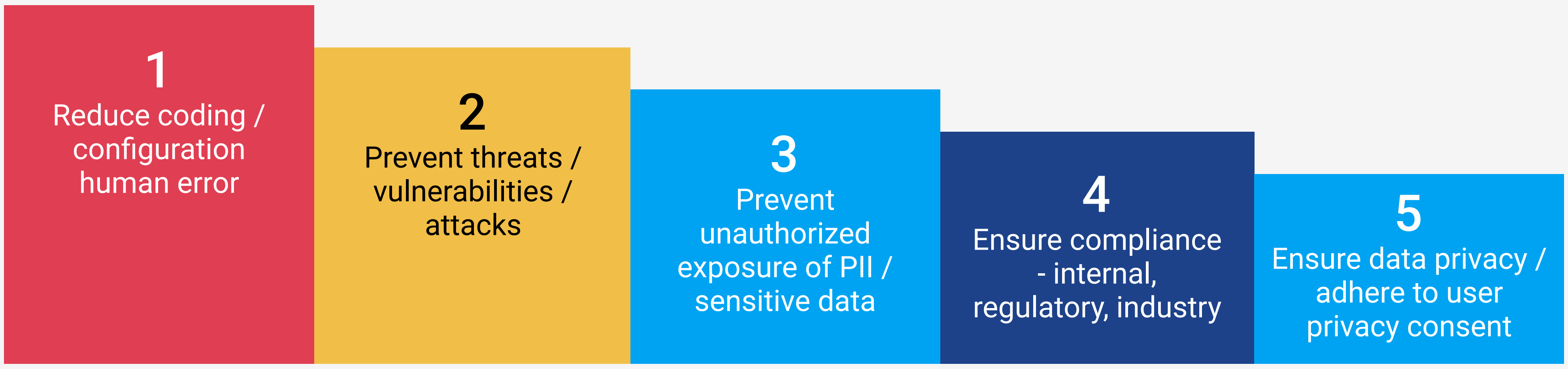
"Over the next 12 months, my company's secure API development / authorization governance programs will become more_____"



Drivers

Other than to reduce coding and human error, the top reasons organizations are initiating or augmenting a secure API development or API security program have to do with preventing threats and unauthorized sensitive data exposure, **as well as ensuring compliance and privacy consent.**

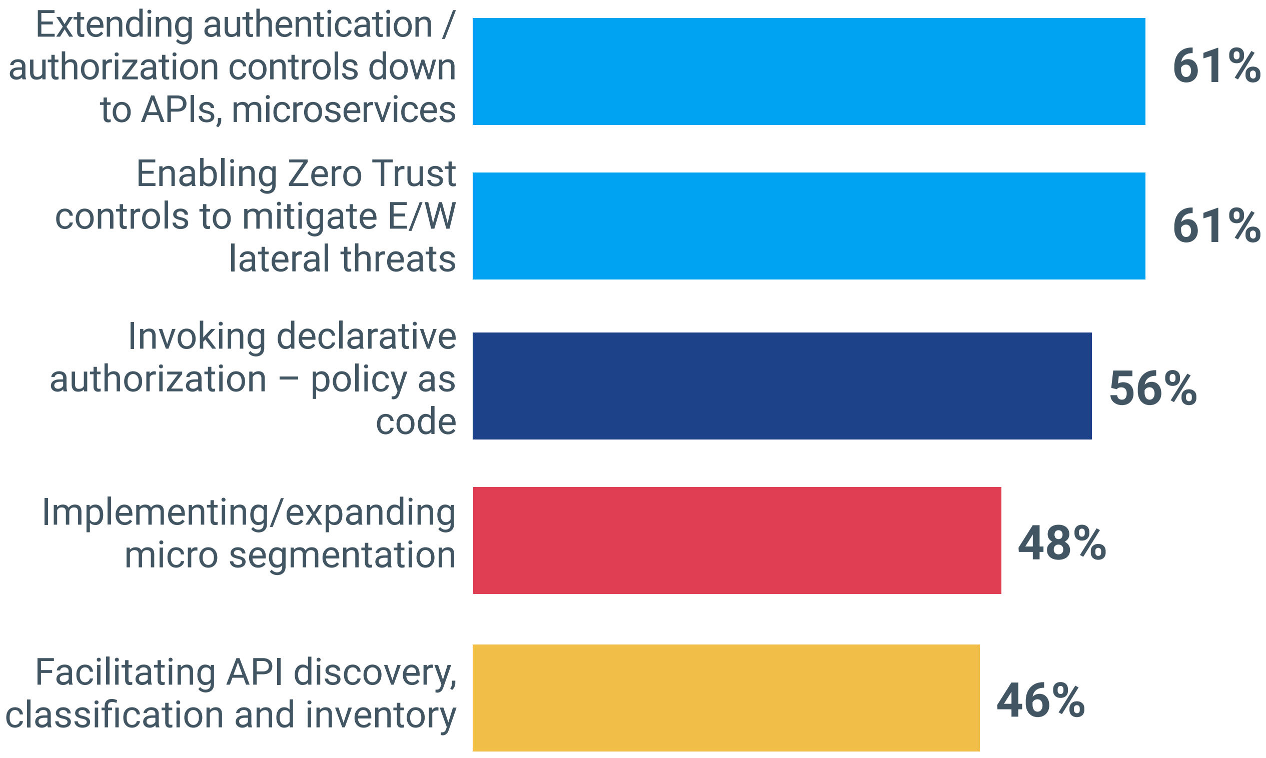
What are the top 5 most critical drivers behind your organization initiating/augmenting a secure API development / API security program?



Initiatives

Most organization’s current or near-term API security and data protection investment priorities are to extend authentication and authorization controls down to APIs, enable zero trust controls to mitigate lateral threats, and invoke declarative authorization.

What are your organization’s current or near-term API security and data protection investment priorities?



Improving OAuth scope definition and enforcement (app, container) **40%**

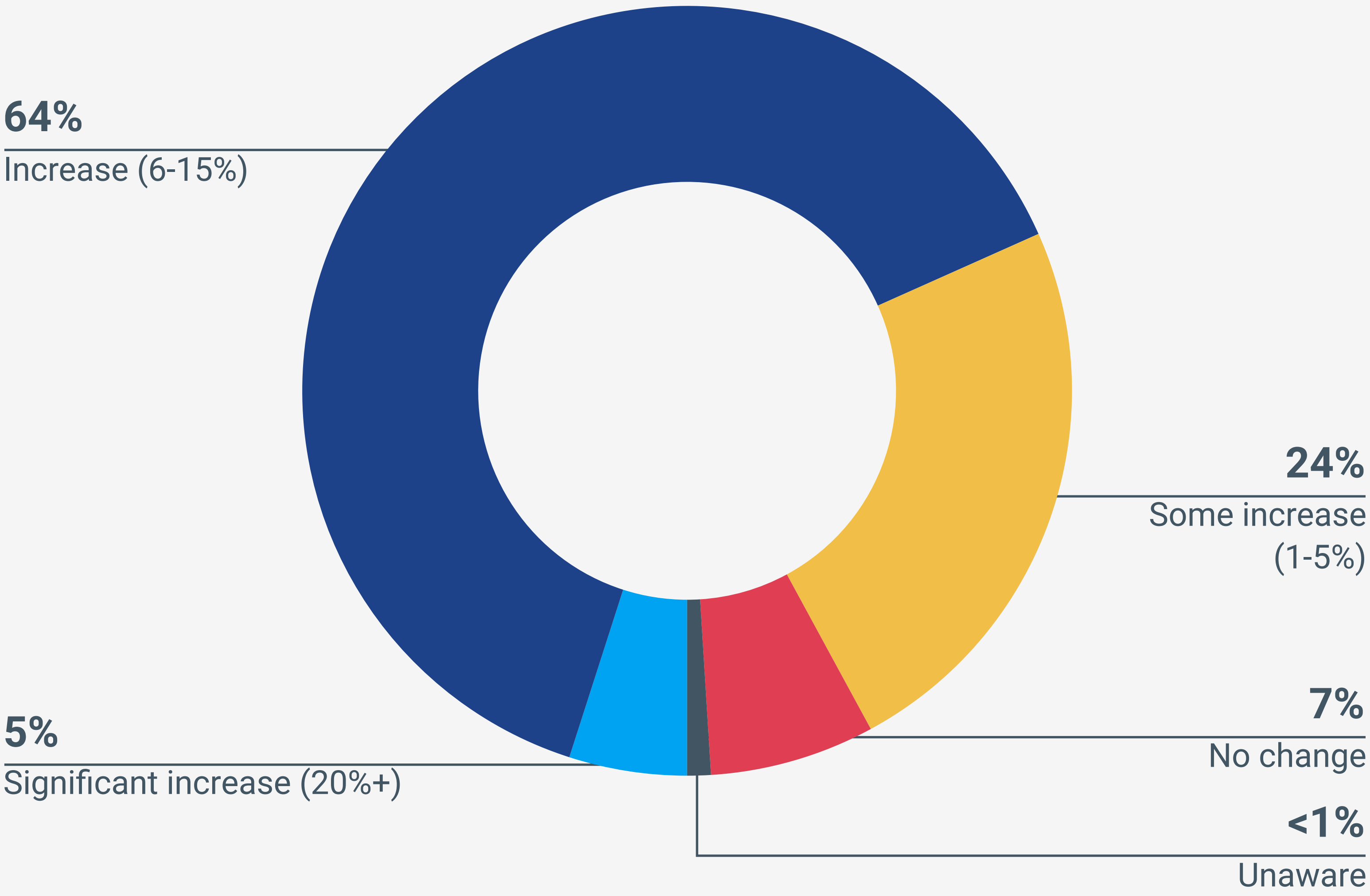
Externalizing authentication and authorization (removing from hard-coding) **37%**

Enabling privacy consent management (user-defined data sharing permissions) **35%**

Investment

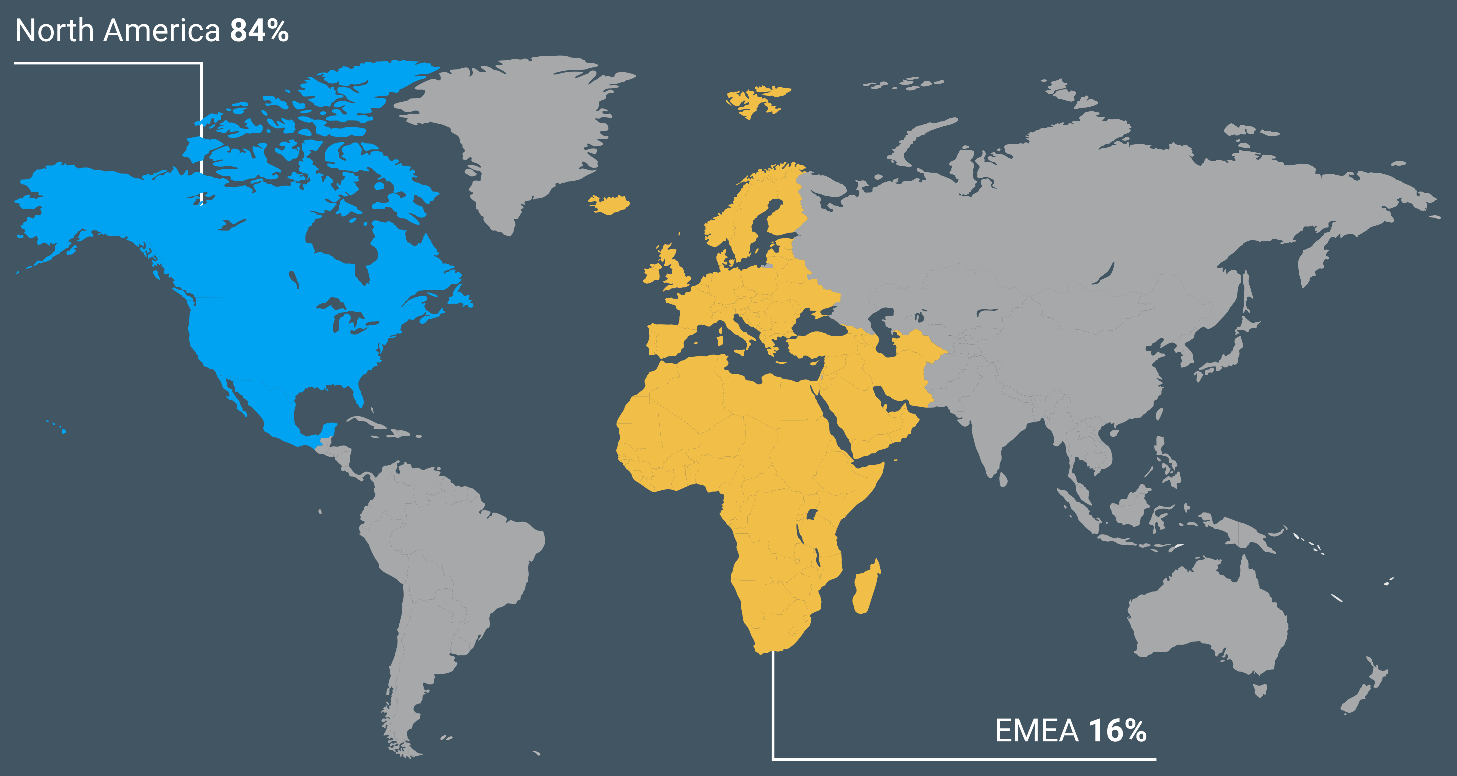
93% of decision-makers report that there will be an increase in budget and resources to their company's secure API development and API security programs over the next 12 months, with **64% increasing between 6% and 15%**.

Over the next 12 months, what investment change in budget and/or resources do you anticipate will be applied to your company's secure API development / API security programs?

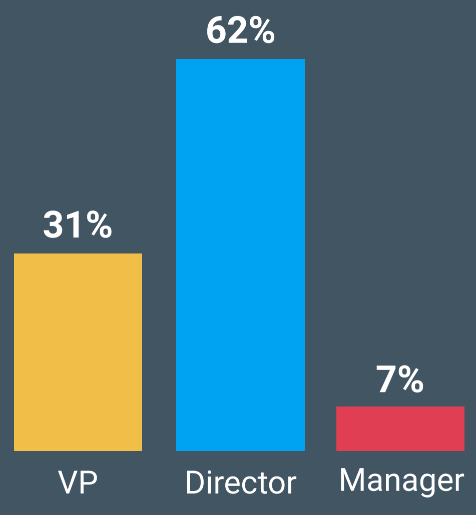


Complete Survey Respondent Breakdown

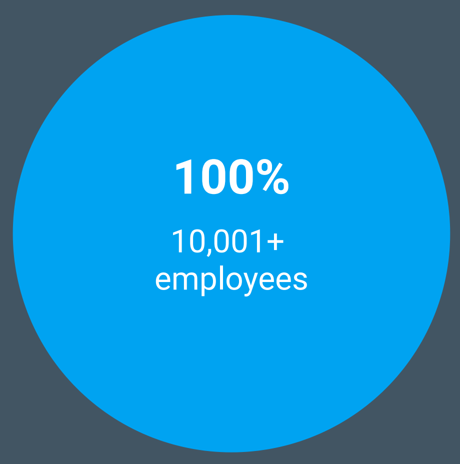
Region



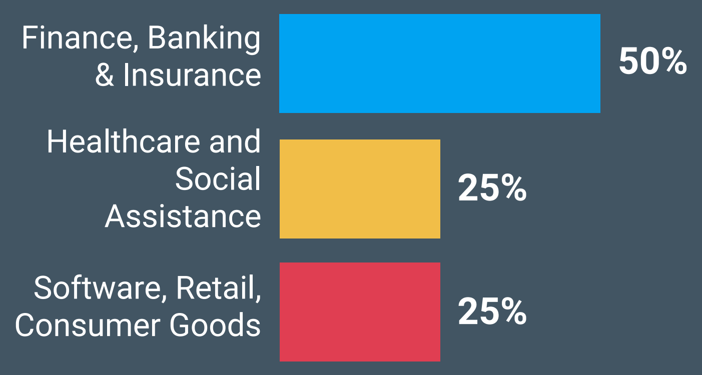
Titles



Company Size



Industry



CLOUDENTITY