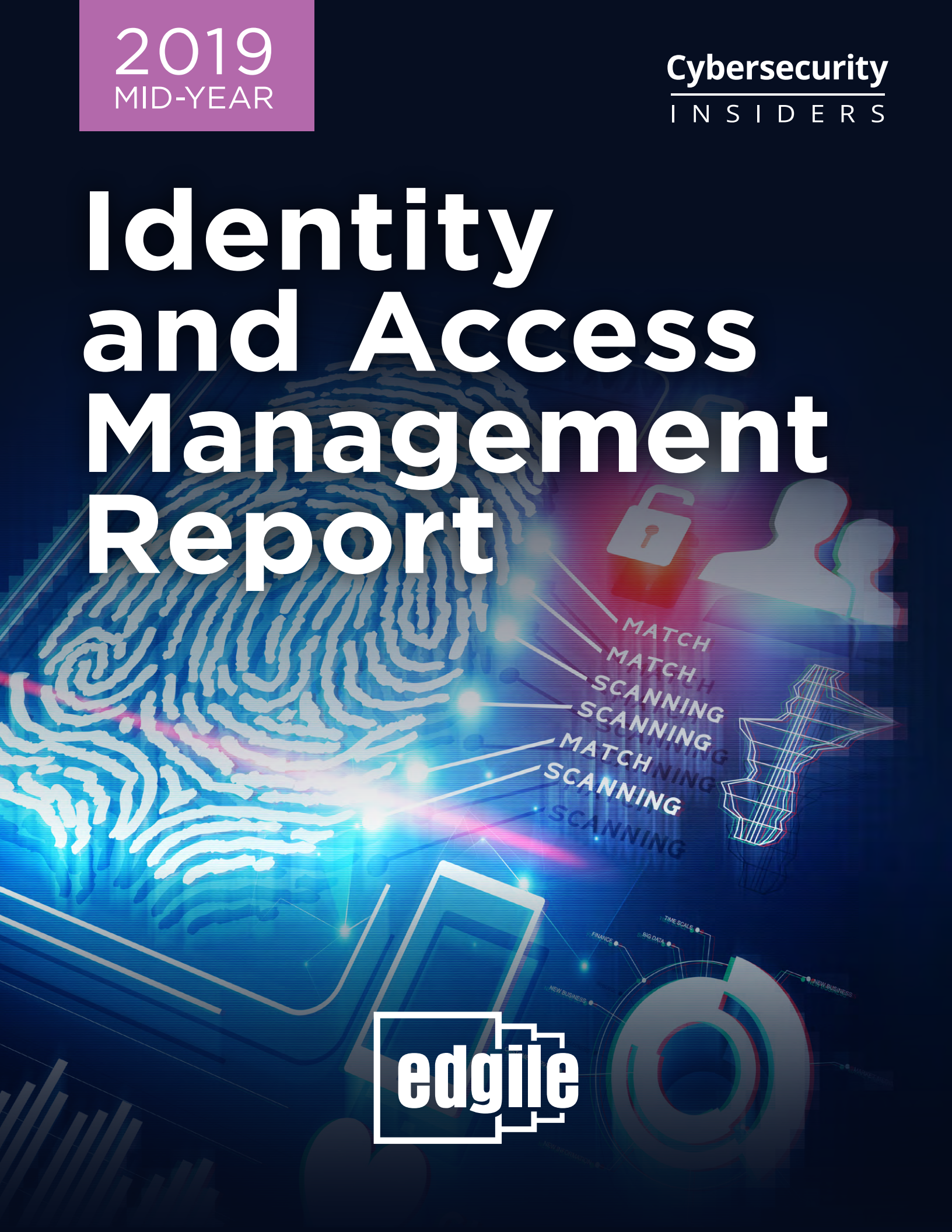
2019
MID-YEAR

Cybersecurity
INSIDERS

Identity and Access Management Report



edgile

INTRODUCTION

The 2019 Identity and Access Management Report reveals the increasing importance of managing access for a significant majority of organizations (86%) as part of their overall risk management and security posture. At the same time, a majority of organizations (53%) are, at best, only somewhat confident in the effectiveness of their identity and access management program.

In the context of this survey report, the purpose of Identity and Access Management is to grant access privileges for the right enterprise assets to the right users in the right context of their role or scope of responsibilities within an organization.

The 2019 Identity and Access Management Report highlights what is and what is not working for security operations teams in securing access to their sensitive data, systems, and applications:

- 70% of organizations have at least a few users with more access privileges than required for their job.
- 66% view role-based access control as most important to them.
- 75% of organizations using IAM saw a reduction of unauthorized access incidents.
- 49% deem identity management and governance, multi-factor authentication, and privileged access management as a priority for IAM investment in the next 12 months.

This 2019 Identity and Access Management Report has been produced by Cybersecurity Insiders, the 400,000 member information security community, to explore the latest trends, key challenges, gaps and solution preferences for Identity and Access Management (IAM).

Many thanks to Edgile for supporting this important research project.

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

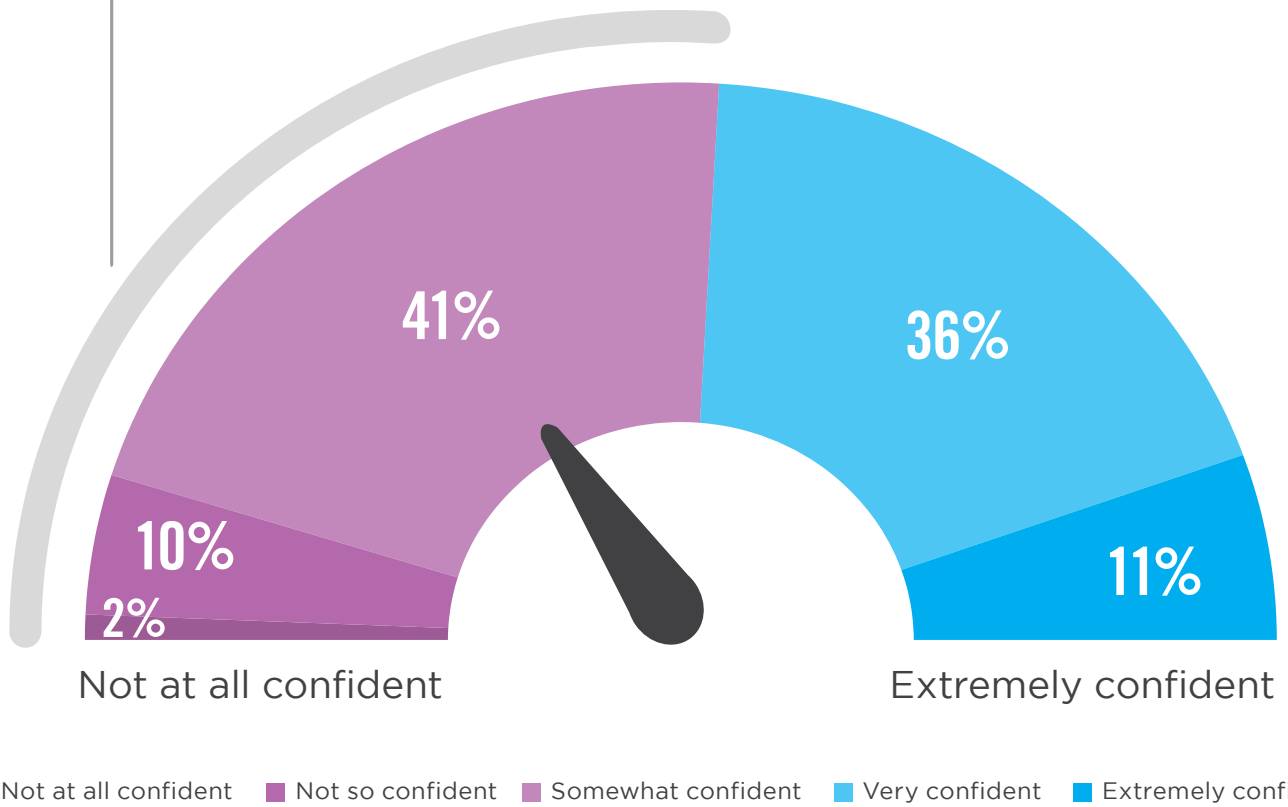
Cybersecurity
INSIDERS

IAM PROGRAM EFFECTIVENESS

A majority of organizations (53%) are, at best, only somewhat confident in the effectiveness of their identity and access management program. Forty-seven percent are very confident to extremely confident.

How confident are you in the effectiveness of your organization's Identity and Access Management program?

53% of organizations are, at best, only somewhat confident in the effectiveness of their identity and access management program.

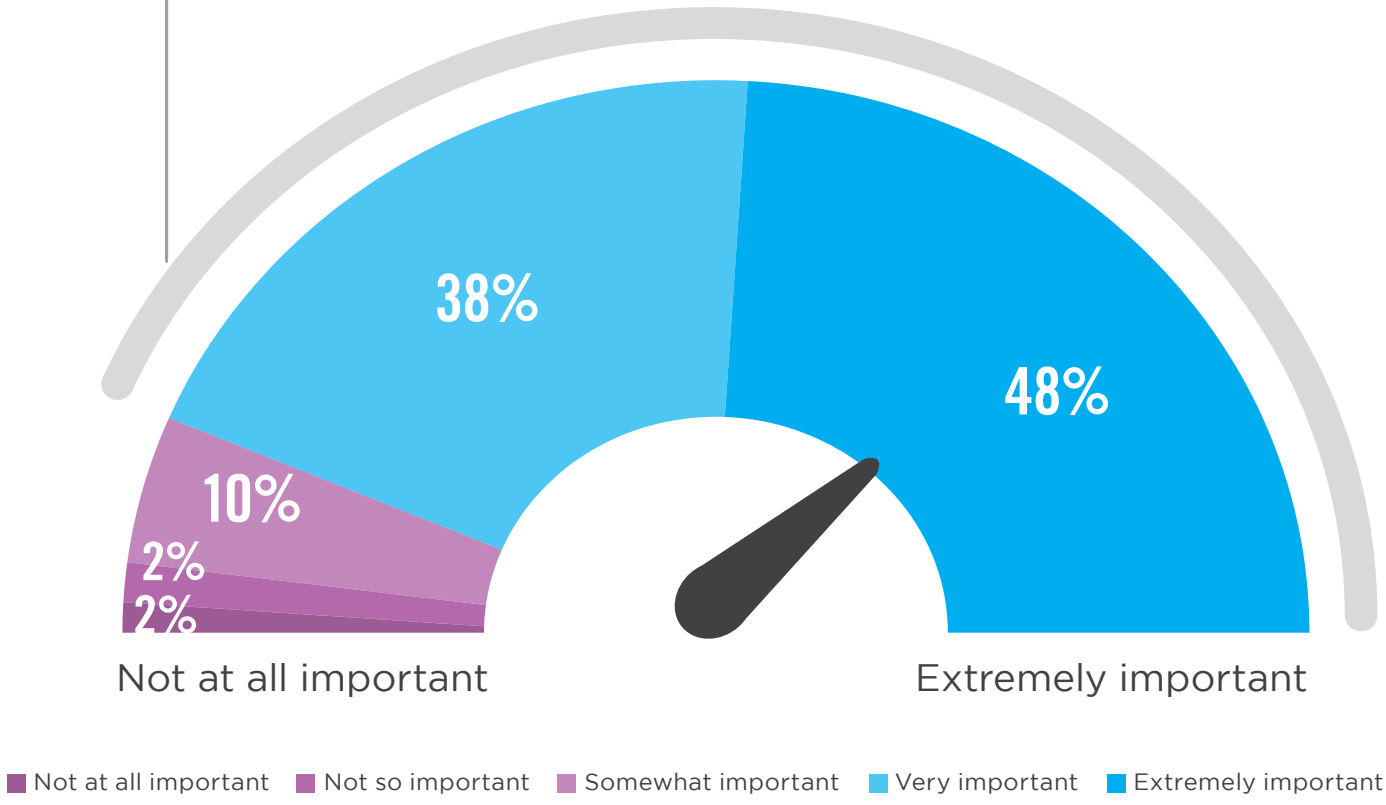


IMPORTANCE OF IAM

Identity and access management is very important to extremely important to a significant majority of organizations (86%) as part of their overall risk management and security posture.

How important is identity and access management to your organization's overall risk management and security posture?

86% of organizations think IAM is very important to extremely important.



IAM CAPABILITIES

The most frequently deployed IAM capabilities include role-based access control (68%), followed by single sign-on (57%) and self-service password management (50%).

What IAM capabilities are deployed in your organization?

68%

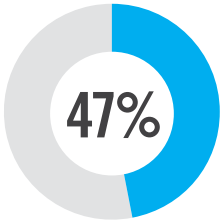
Role-based access control

57%

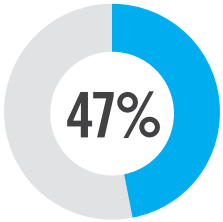
Single sign-on

50%

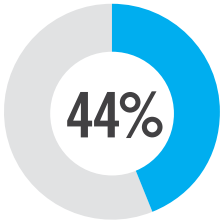
Password self-service



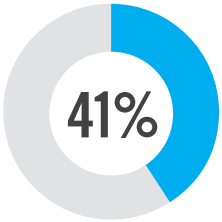
Compliance or auditor reporting



User monitoring



Administrative reporting



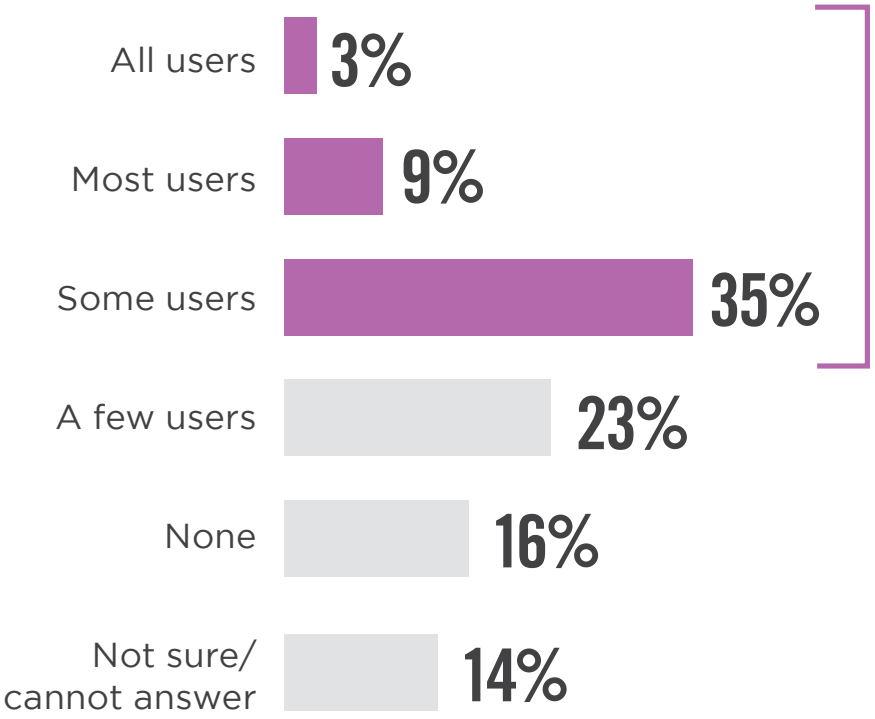
System & application access monitoring

Automated user provisioning/de-provisioning 38% | Integration with service desk/ITSM solutions 36% | Considerations for contract or temporary staff 31% | Streamlined user certification/auditing 26% | Advanced analytics (such as Artificial Intelligence (AI) or Machine Learning (ML)) 12% | Other 7%

EXCESSIVE ACCESS PRIVILEGES

About half of organizations (47%) report that at least some users (35%), most users (9%) or all users (3%) have more access privileges than required for their job.

How many users in your organization might have more access privileges than required for their job?



47%

of users have at least some users with more access privileges than required for their job.

KEY DRIVERS FOR IAM

Organizations prioritize security (68%) over operational efficiency (49%) and breach prevention (45%) as the key drivers for developing an IAM program.

What were the key drivers for your organization's initial development of an identity and access management program?

68%

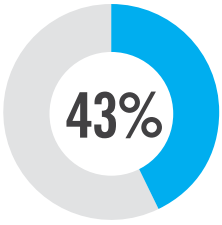
Security

49%

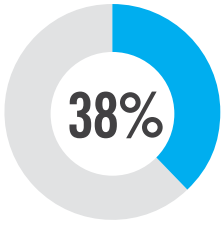
Operational efficiency

45%

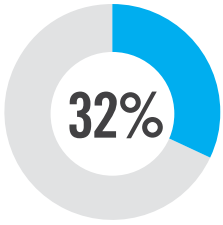
Breach prevention



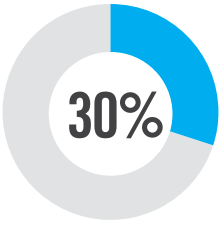
Compliance with internal mandates



Response to regulation or industry standards (HIPAA, GDPR, etc.)



Response to a security incident or audit finding



Insider threats

Poor user experience 17% | Not applicable/We do not have an Identity and Access Management program 5% | Other 8%

ACCESS CONTROL PRIORITIES BY SYSTEM

When it comes to prioritization of systems to protect through robust access control, a majority of organizations focus on enterprise applications (67%), web/cloud apps (64%), and servers (59%).

Which systems in your organization most require robust access control?

67%

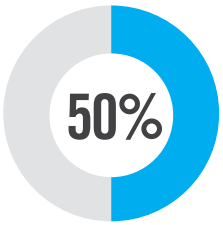
Enterprise applications

64%

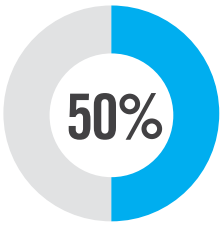
Web apps/ cloud apps

59%

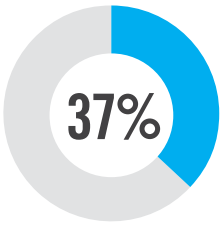
Servers



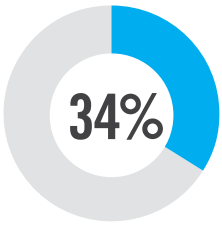
Local network



VPN



Desktops/ laptops



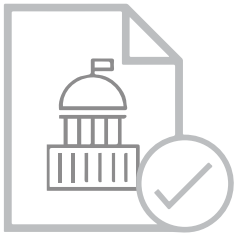
Mobile devices and apps

Other 6%

IAM INVESTMENT PRIORITY

Over the next 12 months, organizations equally prioritize multi-factor authentication (49%), identity management and governance (49%) and privileged access management (49%).

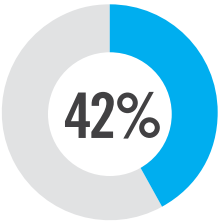
Which of the following areas is a priority for IAM investment in your organization in the next 12 months?



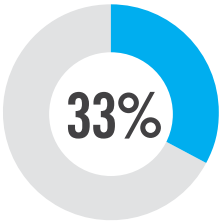
49%
Multi-factor authentication

49%
Identity management and governance

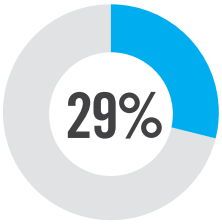
49%
Privileged access management



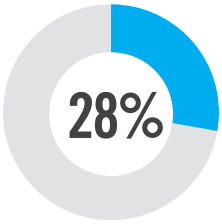
Single sign-on & federation



Network access control



Virtual Private Networks (VPN)



Cloud Access Security Broker (CASB)

Identity analytics 27% | Web application firewall 19% | Enterprise directory 16% | Software Defined Perimeter (SDP) 9% | Other 9%

AUTHENTICATION METHODS

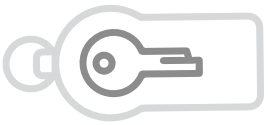
Not surprisingly, by far the most popular authentication method is username and password (86%), followed by software tokens (43%) and hardware tokens (38%).

What authentication methods are used in your organization?

86% Username and password

43%

Software tokens (e.g. One Time Password (OTP))



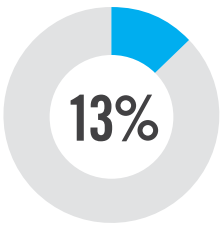
38%

Hardware tokens (e.g. key fobs, USB tokens, smart cards)

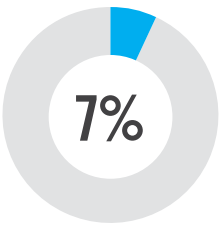
25%

Biometric authentication

Out-of-band authentication (e.g. Push, SMS, voice, etc.)



Tokenless authentication (e.g. context-based authentication and pattern-based authentication)



Social identity credentials (e.g. using LinkedIn, Facebook, Twitter, etc.)

Other 3%

CRITICAL CAPABILITIES

Organizations in our survey prioritize role-based access control as the most critical IAM capability (66%), followed by single sign-on (59%) and system and application access monitoring (50%).

What IAM capabilities are most important to you?

66%

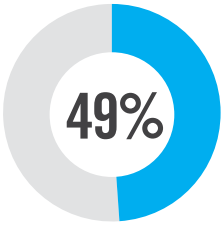
Role-based access control

59%

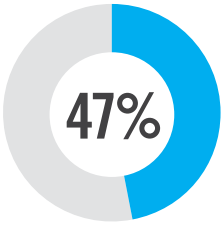
Single sign-on

50%

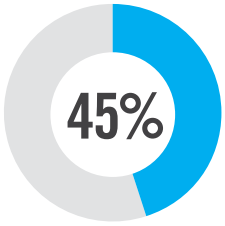
System & application access monitoring



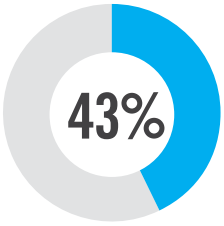
Compliance or auditor reporting



Automated user provisioning/ de-provisioning



Password self-service



Administrative reporting

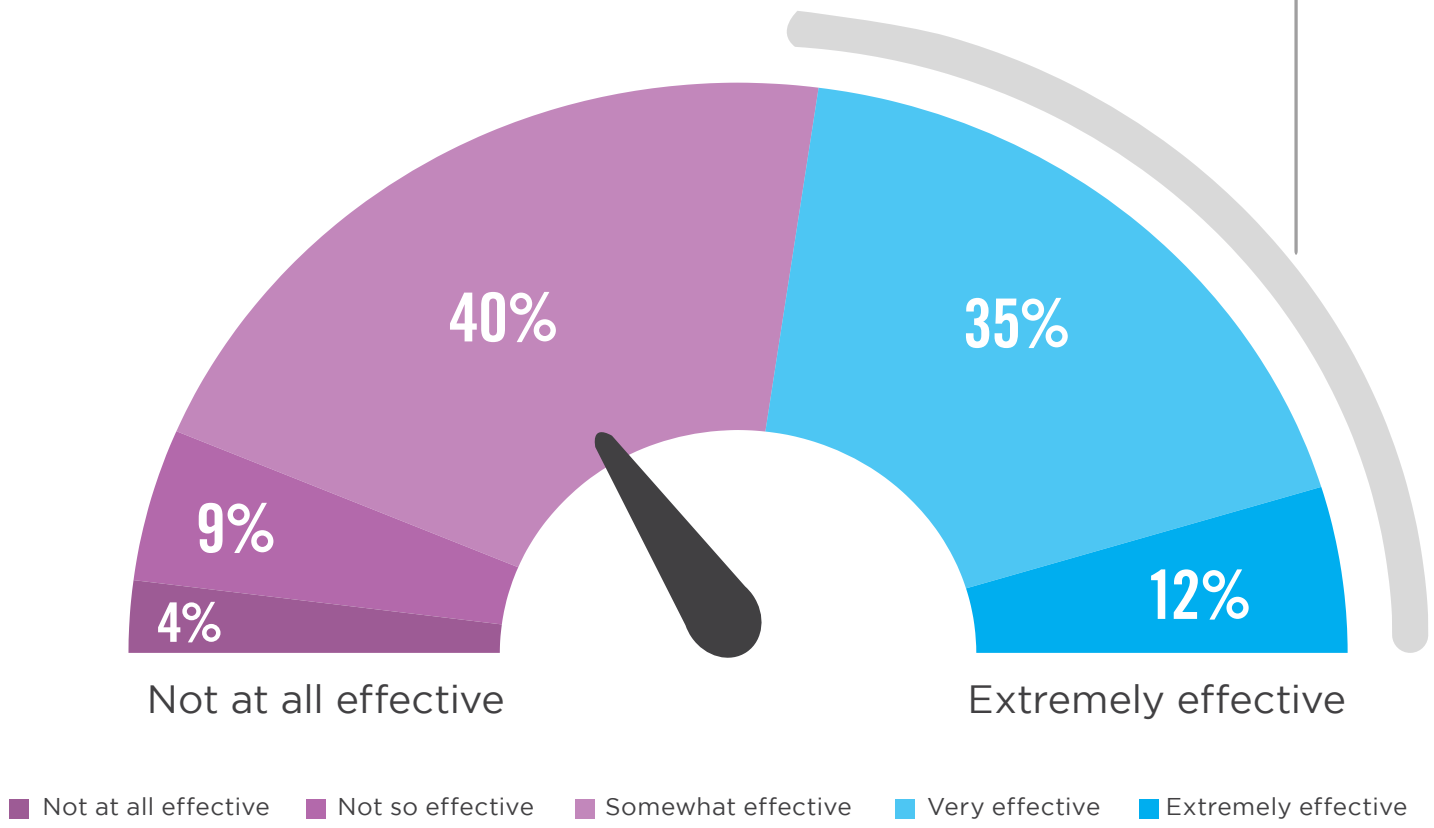
Support of compliance requirements 42% | User monitoring 36% | Streamlined user certification/auditing 33% | Workflow and case management 30% | Access request dashboards 23% | Considerations for contract or temporary staff 23% | Advanced analytics (such as Artificial Intelligence (AI) or Machine Learning (ML)) 22% | Ability to personalize platform 20% | Other 3%

ACCESS MANAGEMENT EFFECTIVENESS

Only less than half of organizations (47%) rate themselves very effective or extremely effective in managing access to sensitive information, applications and systems.

How would you rate your organization's effectiveness in managing access to sensitive information, applications and systems?

Of organizations rate themselves very effective or extremely effective in managing access to sensitive information, applications and systems. **47%**



REDUCTION OF UNAUTHORIZED ACCESS

For 75% of organizations, utilizing identity and access management solutions has resulted in a reduction of unauthorized access incidents. Only a small fraction of 6% report no improvement.

How has using IAM solutions changed the occurrence of unauthorized access in your organization?

75%

of organizations using IAM saw a reduction of unauthorized access incidents.

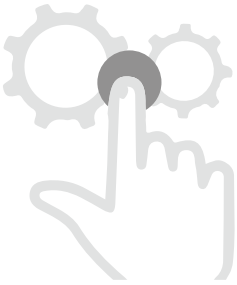
KEY CHALLENGES

Lack of skilled staff (43%) and having to manually create and refine access rules and roles (43%) are tied for the biggest challenge organizations are facing when managing access to sensitive systems, applications and data.

What are the key challenges for managing access in your organization?

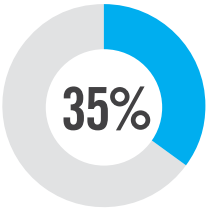
43%

Lack of skilled staff

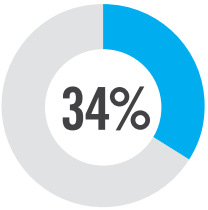


43%

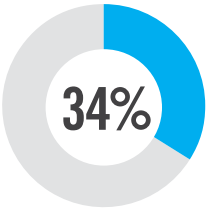
Lack of automation/having to manually create and refine access rules and roles



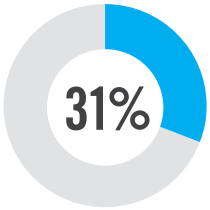
Password management and authentication



Not utilizing proper technologies



Detection and/or mitigation of insider threats (negligent, malicious, and compromised users)



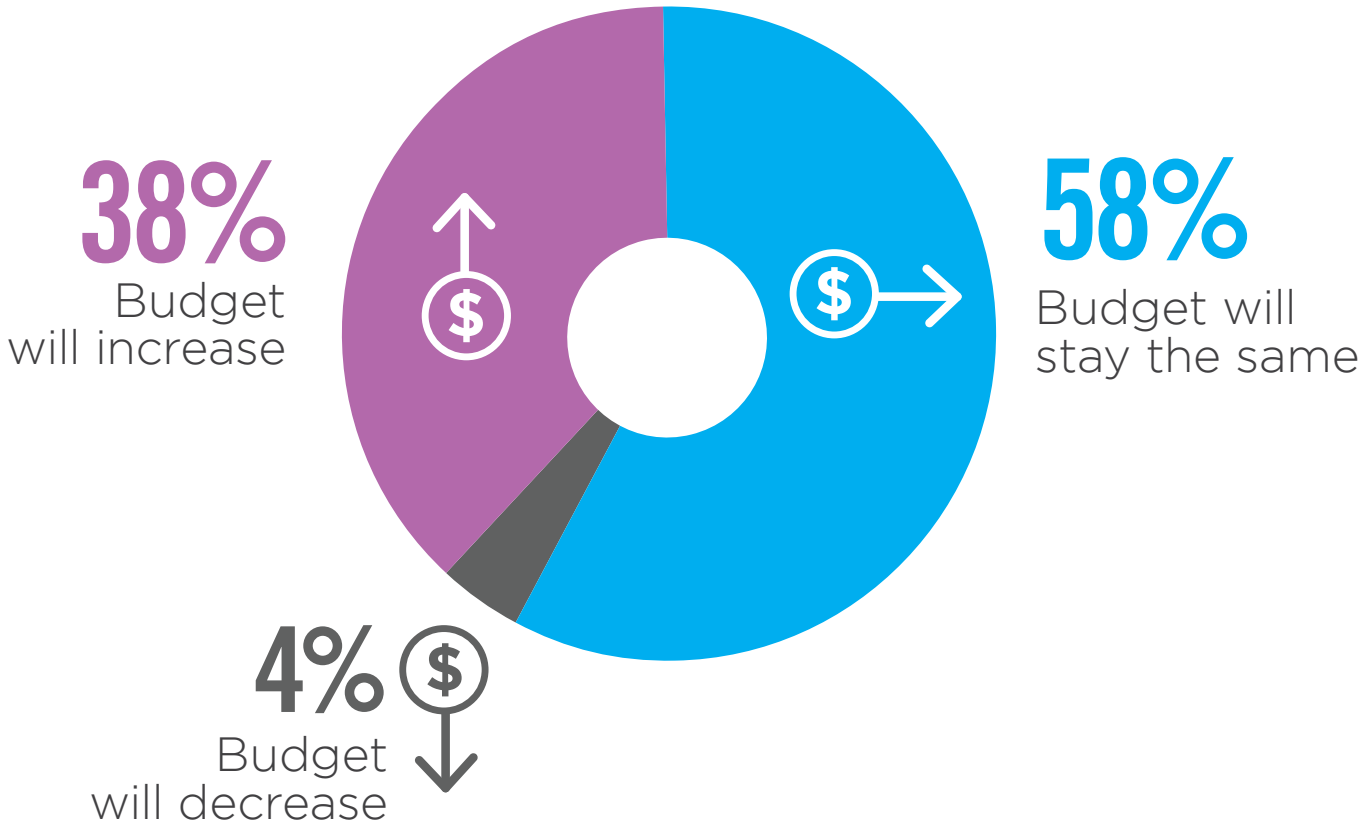
Increasing number of regulations and mandates

User/staff turnover 31% | Increasing use of mobile devices 29% | Lack of budget 29% | Migration to the cloud 28% | Poor integration/interoperability between security solutions 28% | Lack of clearly defined access policies and procedures 27% | Difficulty implementing and deploying a solution 25% | Lack of security awareness/compliance among employees 25% | Changes to the organization (due to re-organization, acquisition, etc.) 20% | Application sprawl 20% | Evolving threat landscape 20% | Reviewing and approving user roles 20% | Lack of proper reporting tools 19% | Poor vendor support 17% | Lack of management support 12% | Lack of effective IAM solutions available in the market 8% | Other 6%

BUDGET TREND

On balance, IAM budget will increase for 38% of organizations that participated in the survey. Only 4% report a planned budget reduction over the next 12 months.

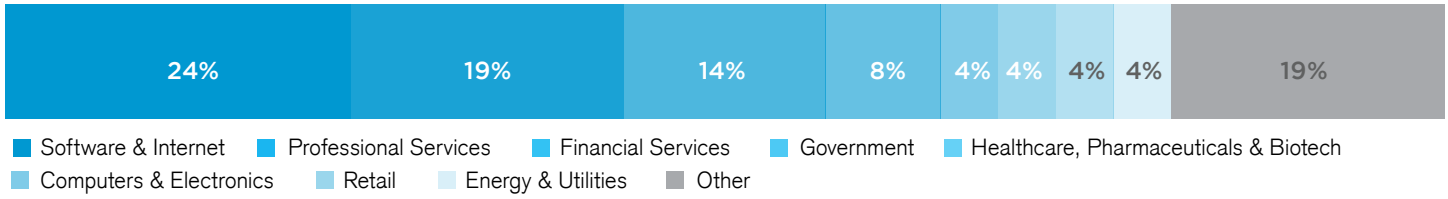
How do you expect your organization's access management related budget to change over the next 12 months?



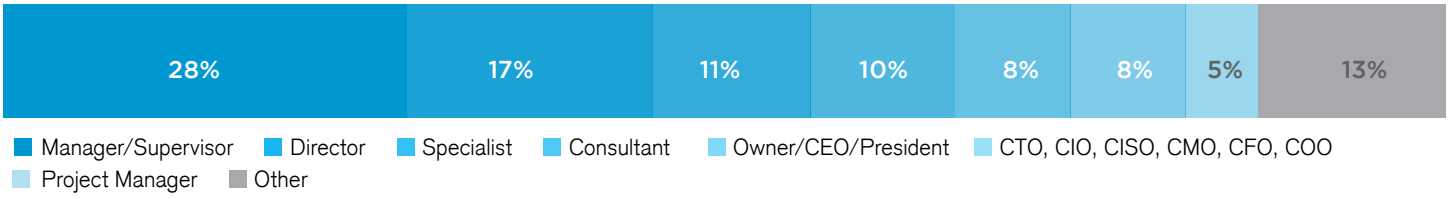
METHODOLOGY & DEMOGRAPHICS

This Identity and Access Management is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in June of 2019 to gain deep insight into the latest trends, key challenges and solutions for identity and access management. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

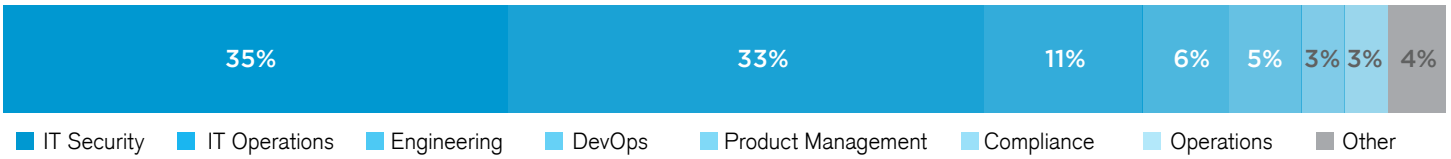
INDUSTRY



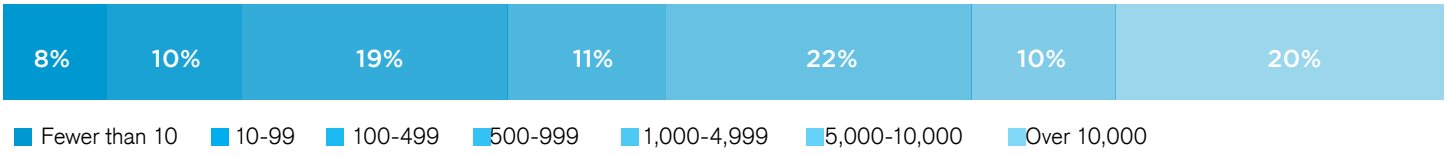
CAREER LEVEL



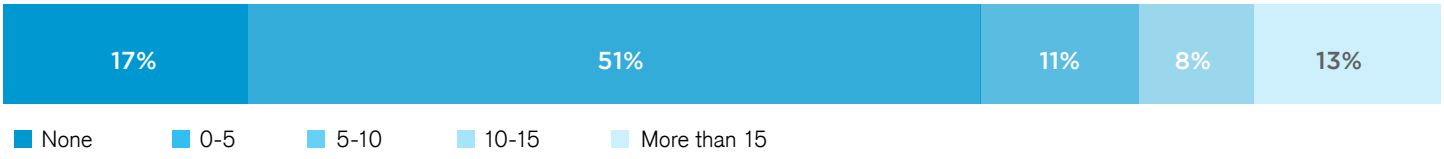
DEPARTMENT



COMPANY SIZE



STAFF DEDICATED TO IAM



Edgile is the trusted cyber risk and compliance partner to the world's leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

Edgile.com