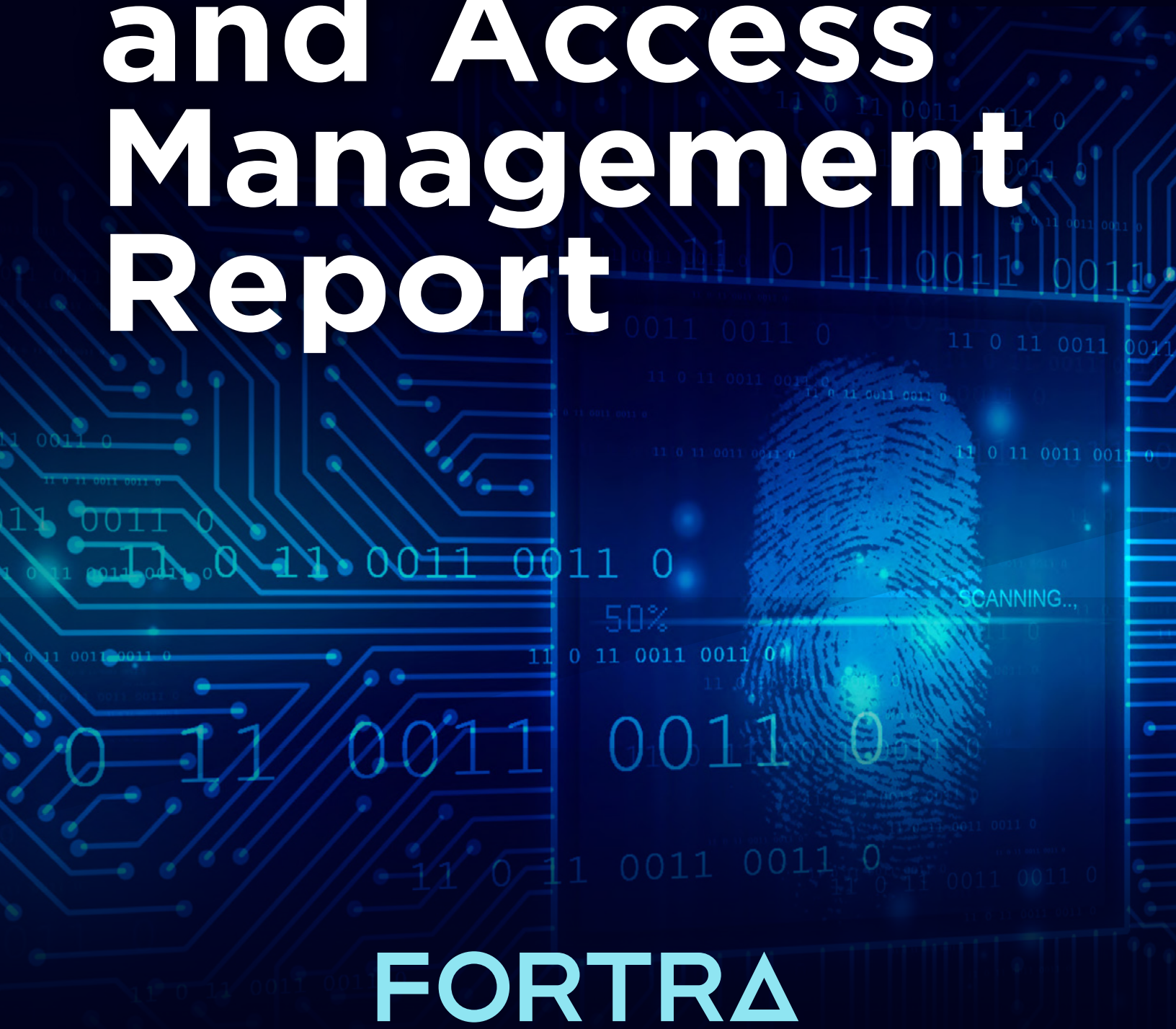
2021

Cybersecurity
INSIDERS

Identity and Access Management Report



FORTRA

INTRODUCTION

The recent, massive shift to remote work has increased organizational risk of insecure access to sensitive data and systems. The 2021 Identity and Access Management Report reveals the increasing importance of managing access as part of an organization's overall risk management and security posture in the new normal of hybrid work locations.

The report highlights what is and what is not working for security operations teams in securing access to sensitive data, systems, and applications.

Key findings include:

- Eighty-seven percent view IAM as very to extremely important to their risk management and security posture.
- Seventy-seven percent have at least a few users with more access privileges than required for their jobs.
- Organizations prioritize role-based access control as the most critical IAM capability (60%), followed by single sign-on (53%) and compliance reporting (51%).
- Seventy-six percent of organizations saw a reduction in unauthorized access from using an IAM solution.

The 2021 Identity and Access Management Report has been produced by Cybersecurity Insiders, the 500,000-member information security community, to explore the latest trends, key challenges, gaps, and solution preferences for Identity and Access Management (IAM).

Many thanks to Core Security, by Fortra, for supporting this important research project.

We hope you 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

IMPORTANCE OF IAM

The dramatic rise in remote work is putting increased pressure on IT and security organizations to manage access to sensitive data and systems. This is reflected in the survey responses, with nearly nine out of ten organizations confirming that Identity and Access Management is very or extremely important to their cybersecurity and risk management posture (87%).

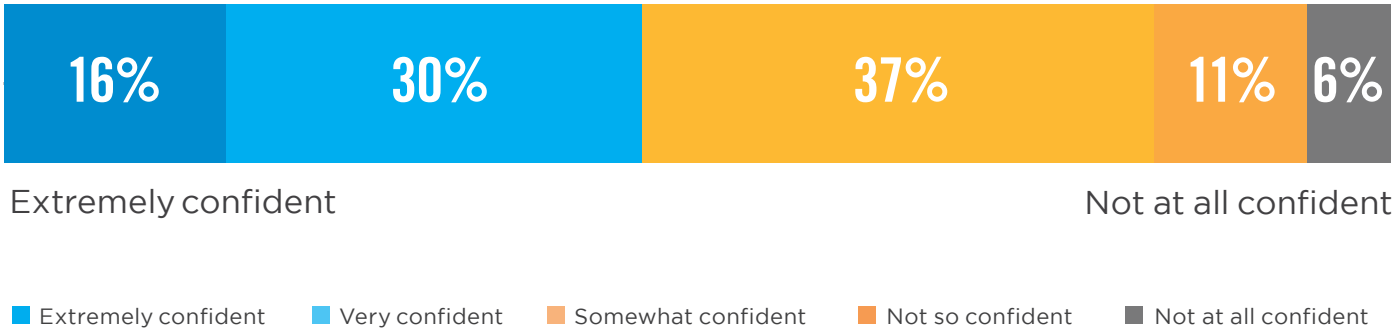
How important is identity and access management to your organization's overall risk management and security posture?

IAM PROGRAM CONFIDENCE

While the importance of IAM is high, organizations' confidence in the effectiveness of their current identity and access management program is relatively low. Fifty-four percent are, at best, only somewhat confident in the effectiveness of their identity and access management program.

How confident are you in the effectiveness of your organization's identity and access management program?

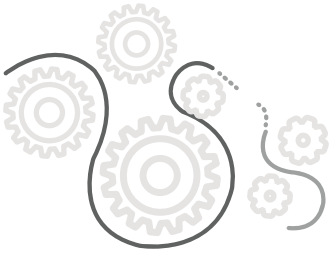
54% of organizations are, at best, only somewhat confident



BUSINESS IMPACT

Failing access and identity controls comes at a high cost: organizations that experienced unauthorized access to sensitive systems and data reported disrupted business activities (22%), system downtime (21%), and reduced employee productivity (20%).

What negative impact did your business experience from unauthorized access to sensitive data, applications, or systems in the past 12 months?

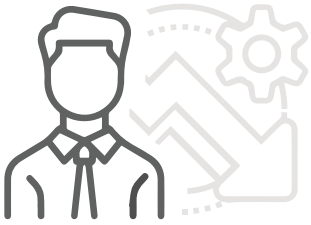


22%

Disrupted business activities

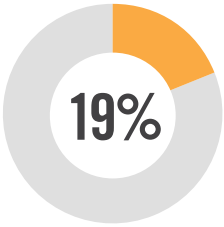
21%

System downtime

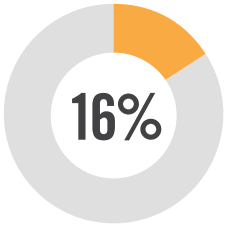


20%

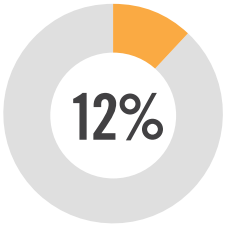
Reduced employee productivity



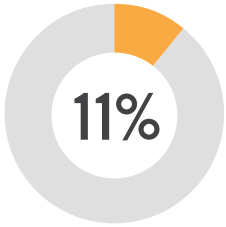
Deployment of IT resources to triage and remediate issue



Increased helpdesk time



Data loss



Loss/compromise of intellectual property

Negative publicity/reputational damage 9% | Reduced revenue/lost business 9% | Lawsuit/legal issues 8% | Customer loss 7%
None/no unauthorized access was known to occur 7% | Regulatory fines 3% | Other 4%

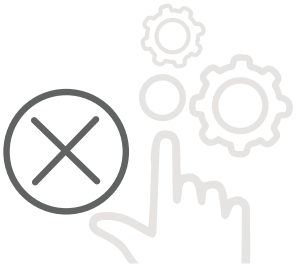
KEY CHALLENGES

We asked organizations what is holding them back in terms of managing secure access. This sentence should say - Lack of skilled staff (38%) and lack of automation (38%) lead the list of key challenges, following by lack of budget (34%).

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

38%

Lack of skilled staff



38%

Lack of automation

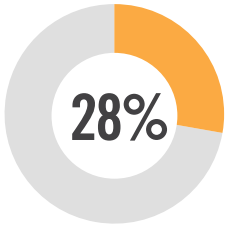
34%

Lack of budget

Not utilizing proper technologies

Migration to the cloud

Increasing use of mobile devices



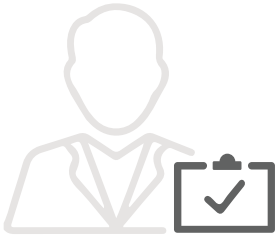
Difficulty implementing and deploying a solution

Detection and/or mitigation of insider threats (negligent, malicious, and compromised users) 25% | Evolving threat landscape 24% | Increasing number of regulations and mandates 23% | Poor integration/interoperability between security solutions 23% | User/staff turnover 22% | Password management and authentication 20% | Lack of security awareness/compliance among employees 20% | Poor vendor support 19% | Changes to the organization (due to re-organization, acquisition, etc.) 19% | Application sprawl 16% | Lack of clearly defined access policies and procedures 15% | Lack of proper reporting tools 13% | Reviewing and approving user roles 13% | Lack of management support 12% | Lack of effective IAM solutions available in the market 10% | Other 4%

IAM CAPABILITIES

We asked cybersecurity professionals what capabilities they prioritize when selecting IAM solutions. Role-based access control tops the chart as the most critical IAM capability (60%), followed by single sign-on (53%) and compliance/auditor reporting (51% - jumping to #3 from the #6 spot in last year's survey).

What IAM capabilities are most important to you?



60%

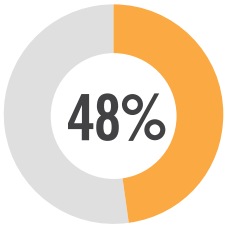
Role-based access control

53%

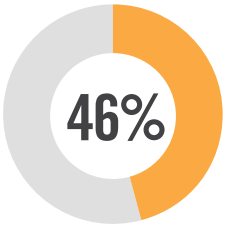
Single sign-on

51%

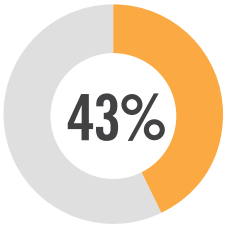
Compliance or auditor reporting



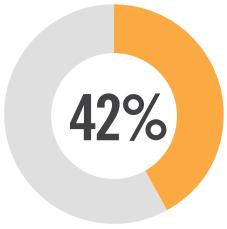
System & application access monitoring



Automated user provisioning/ deprovisioning



Support of compliance requirements



Password self-service

Administrative reporting 40% | Considerations for contract or temporary staff 31% | Streamlined user certification/auditing 29% | Workflow and case management 28% | Advanced analytics (such as artificial intelligence (AI) or machine learning (ML)) 26% | Access request dashboards 25% | Ability to personalize platform 19% | Other 1%

ROLE DESIGN

Role design enables organizations to focus on role definitions and assignments rather than individual accounts and entitlements. Only 48% are, at best, somewhat effective in their current ability to design roles. This is a three percentage point increase over last year's survey, which indicates it's a continuing challenge and likely a reason why role-based access control topped the list of the most important IAM capability.

How effective is your organization's ability to design roles?

An increase of three percentage points from last year

48% of organizations are, at best, only somewhat effective in their ability to design roles

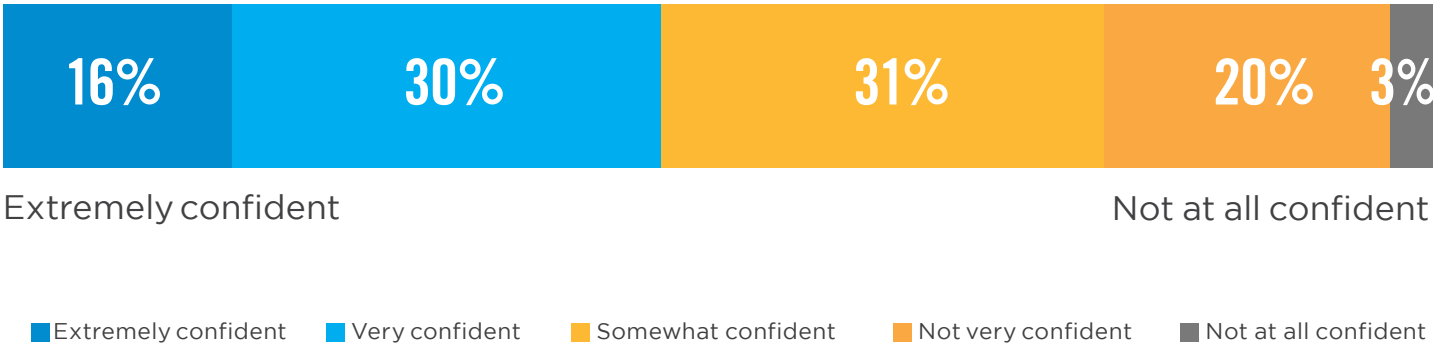
ACCESS PRIVILEGES CONFIDENCE

Determining current access privileges for all users can be a daunting task to make sure users are limited to the appropriate access levels. Only fifty-four percent of organizations are, at best, only somewhat confident in their ability to verify that users do not have excessive access privileges.

How confident are you in your organization's ability to verify that users don't have excessive access privileges?

An increase of four percentage points from last year

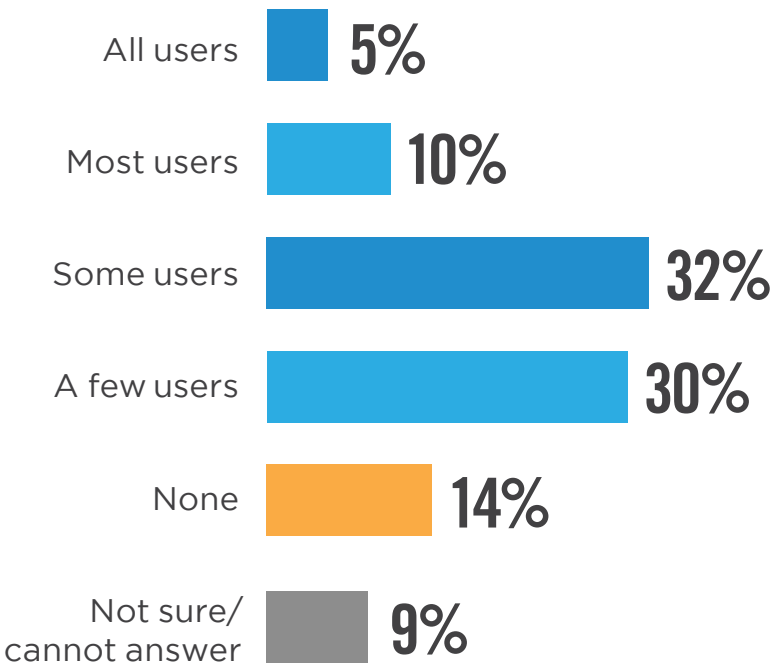
54% of organizations are, at best, only somewhat confident in their ability to verify users access privileges.



EXCESSIVE ACCESS PRIVILEGES

Seventy-seven percent of organizations have at least a few users with more access privileges than required. This is an increase of two percentage points compared to last year.

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



77%

of organizations have at least a few users with more access privileges than required

An increase of two percentage points from last year

KEY DRIVERS

When asked about the key drivers for developing their IAM programs, organizations rank security as the biggest driver (74%), followed by operational efficiency (56%) and breach prevention (44%).

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

74%

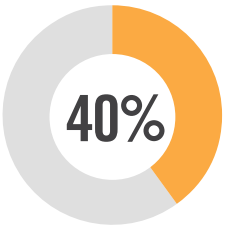
Security

56%

Operational efficiency

44%

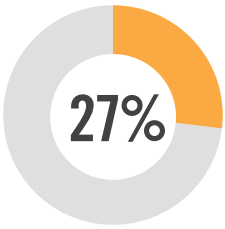
Breach prevention



Compliance with internal mandates

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

Insider threats



Response to a security incident or audit finding

Poor user experience 17% | Not applicable/we do not have an identity and access management program 5% | Other 3%

IAM INVESTMENT

We asked organizations about their IAM investment priorities. Over the next 12 months, organizations continue to prioritize investing in privileged access management platforms (53%). Privileged Access Management (PAM) is a security practice designed to manage privileged access within an organization's IT systems, applications, and infrastructure. It is unsurprising that this is a popular area for investment because many compliance regulations require organizations to have a PAM strategy and technology in place, in addition to the robust security posture it enables. Investment in PAM is followed by multi-factor authentication (52%) and identity management and governance (44%).

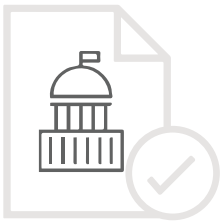
Which of the following areas is a priority for IAM investment in your organization in the next 12 months?

53%

Privileged access management

52%

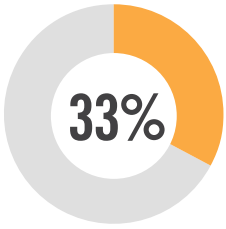
Multi-factor authentication



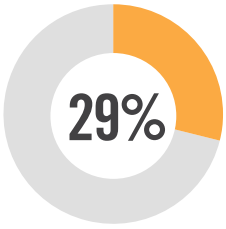
44%

Identity management and governance

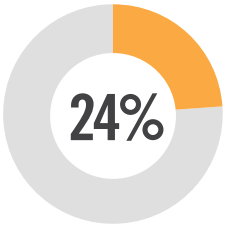
Single sign-on & federation



Network access control



Virtual Private Networks (VPN)



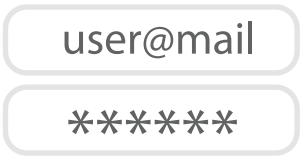
Cloud Access Security Broker (CASB)

Identity analytics 22% | Web application firewall 20% | Enterprise directory 16% | Software Defined Perimeter (SDP) 11% | Other 6%

AUTHENTICATION METHODS

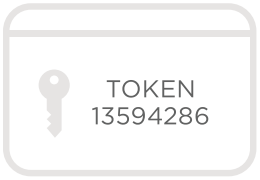
What authentication methods are most used? Not surprisingly, by far the most popular authentication method still is username and password (86%), followed by software tokens (50%) and out-of-band authentication methods, such as text messaging (37%).

What authentication methods are used in your organization?



86%

Username and password

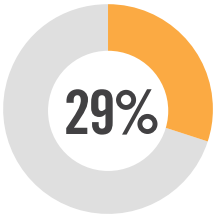


50%

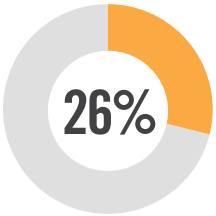
Software tokens (e.g., One Time Password (OTP))

37%

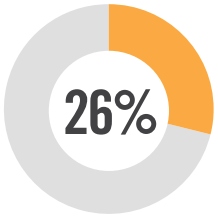
Out-of-band authentication (e.g., Push, SMS, voice, etc.)



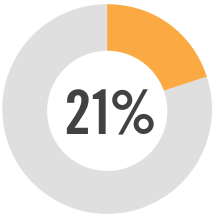
Hardware tokens (e.g., key fobs, USB tokens, smart cards)



Biometric authentication



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



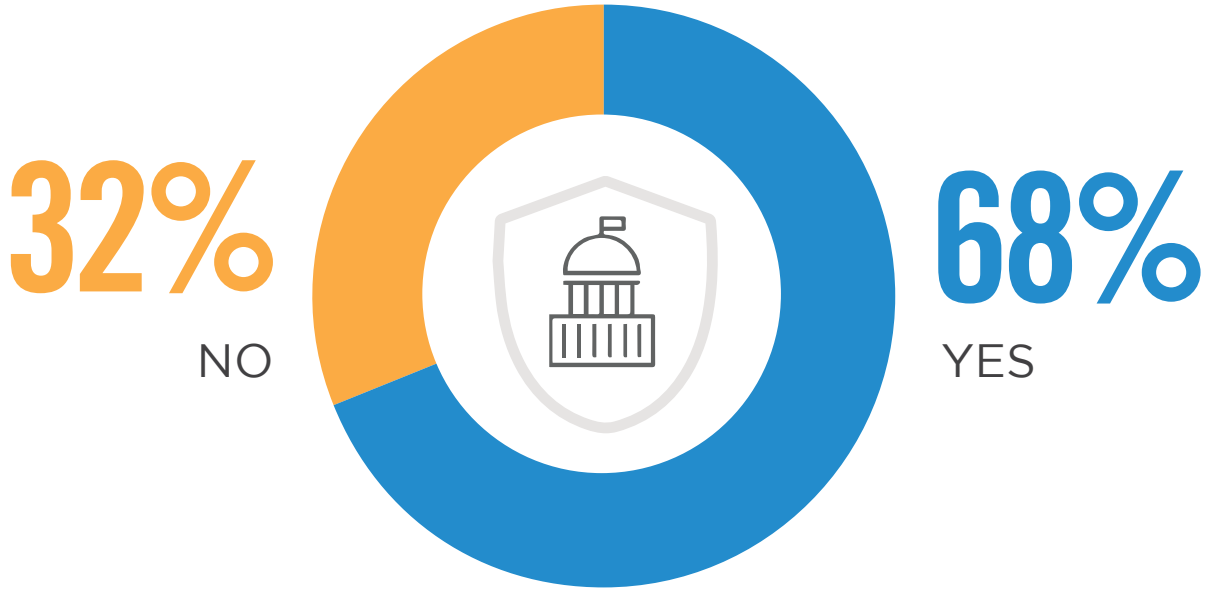
Tokenless authentication (e.g., context-based authentication and pattern-based authentication)

Other 5%

IDENTITY GOVERNANCE

Identity governance and administration policies help define and standardize levels of access rights based on roles or job duties. Most organizations (68%) confirm they are using solutions to address identity governance as part of their IAM strategy to help streamline the provisioning process, adhere to relevant regulations, and provide actionable analytics.

Are you using solutions or tools to address identity governance as part of your IAM strategy?



IMPACT ON UNAUTHORIZED ACCESS

We asked cybersecurity professionals how using an IAM solution has impacted unauthorized access. For 76% of organizations, utilizing identity and access management solutions has resulted in a reduction of unauthorized access incidents. Only a small fraction of 11% report no improvement.

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

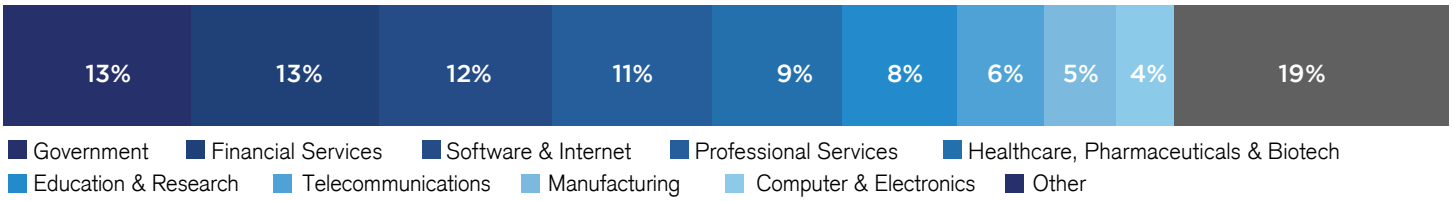
76%

of organizations using IAM saw a reduction of unauthorized access incidents

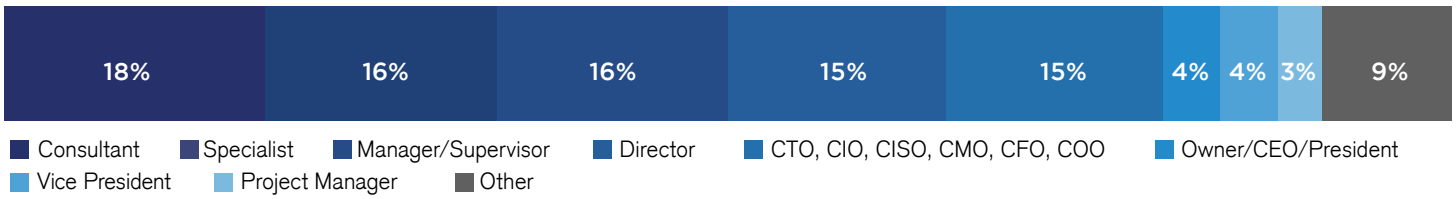
METHODOLOGY & DEMOGRAPHICS

The 2021 Identity and Access Management Report is based on the results of a comprehensive online survey of 338 cybersecurity professionals, conducted in July 2021, 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.

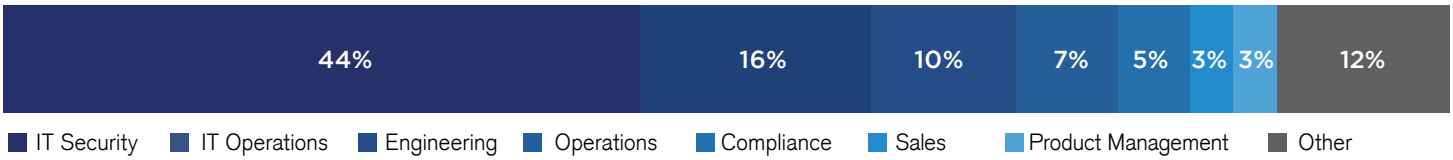
INDUSTRY



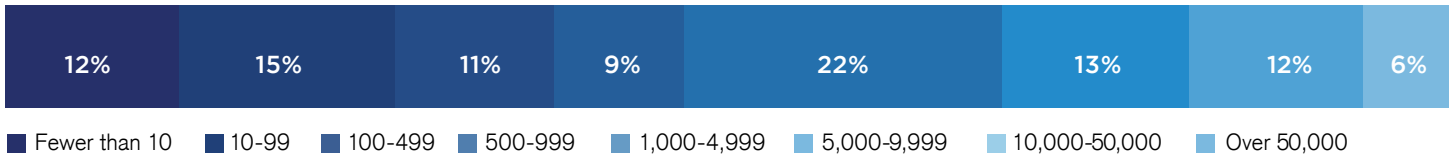
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-cs-gd-1122-r1-79d)