Saviynt

Achieving Continuous Privacy Compliance in Australia

Navigate the regulatory landscape with an identity-first approach

New edition updated for 2024

Contents

Introduction	2
The Current State of Cyber Risk in Australia	2
The Current State of Privacy Laws in Australia	4
Australian Privacy Act	5
Australian Government Information Security Manual	6
Essential Eight Maturity Model	7
Identity and Access Governance: The Privacy Convergence	8
Approaching Compliance Through an Identity-First Lens	9
Five Steps for Maturing and Modernising Data Privacy and Security	10

Contents

Analyse Risk 10

Determine Users 11

Set Controls 11

Monitor Access 12

Document Decisions 12

Intelligent Compliance-as-a-Service with Saviynt 13

Reconcile Roles for a Standardized Authoritative Identity Source 13

Automate Requests, Reviews & Certification to Continuously Monitor Controls 13

Manage Machine Identities for Holistic Access Governance 14

Protect Sensitive & Privileged Access With PAM 14

Introduction

As organisations and agencies consume more cloud resources, they seek automated solutions to help them mitigate the risks arising from these new operational models. New regulations, including the General Data Protection Regulation (GDPR) and the Australian Prudential Standard CPS 234, suggest that organisations should use new technologies to prevent data breaches. Many organisations and agencies that need to meet security and privacy mandates now seek to mitigate risks and mature their cybersecurity posture with solutions that apply artificial intelligence, machine learning, or predictive analytics for greater ecosystem visibility.

As Australian government agencies and companies look to protect constituent and customer data, they need to establish risk-based policies, procedures, and processes and find solutions to maintain the effectiveness of the controls created continuously. This paper will cover the current state of cyber risk, the existing regulatory environment in Australia, and recommended compliance models. We will then discuss how the Saviynt Identity Cloud helps organisations get the benefits of an identity-first approach to mitigating risk and achieving compliance.

The Current State of Cyber Risk in Australia

Cybercriminals continue to evolve their threat methodologies. BDO Australia in conjunction with AusCert, the not-for-profit Cyber Emergency Response team, released the 2022 Cyber Security Report. According to the report:

- There was a 17% increase in the number of organisations who experienced one or more cyber security incidents with a detrimental impact to their operations
- Confidence in managing cyber incidents dropped 11% compared to 2021
- Customer and employee record compromises surged 70% and 54% respectively since 2021
- Attacks damaging brand and business reputation rose by 40%

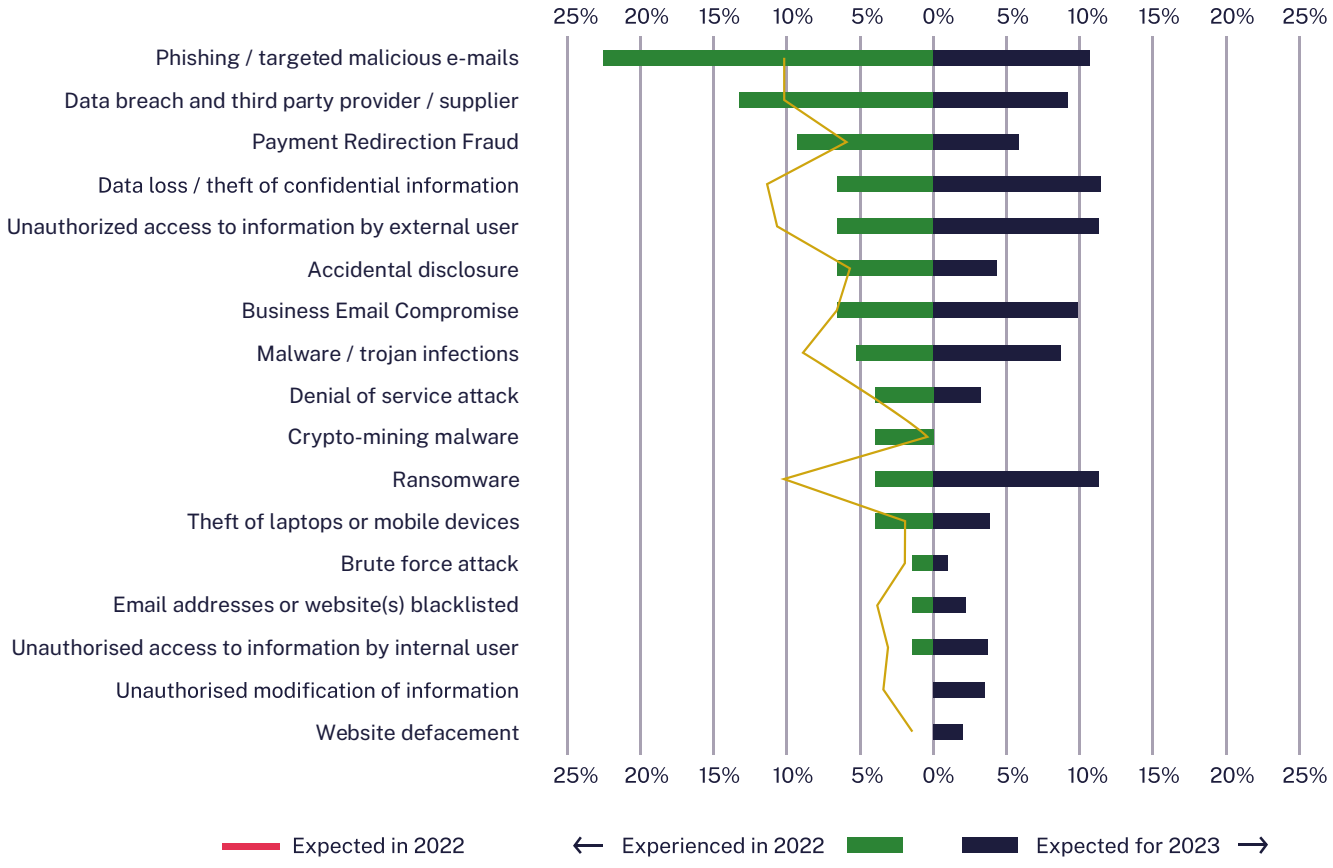
As organisations and agencies move to digital business models, they must establish and enforce appropriate risk-based access controls. While establishing controls is a challenge on its own, continuously monitoring and enforcing these controls becomes downright burdensome – IT staff must review multiple documentation sources and respond to access requests.

Meanwhile, the 2022 Cyber Security Survey indicates that the top five controls for establishing cyber resilience are:

1. Have a clear understanding of the assets and data they possess and the level of sensitivity
2. Establish strong leadership to set direction
3. Implementation of technical controls, including identity and access management
4. Adopt risk management strategies, including cloud security policies to mitigate risk
5. Invest in the necessary resources to detect and respond to cyber incidents

INCIDENTS EXPERIENCED IN 2022 VS. INCIDENTS EXPECTED IN 2023

Source: BDO Australia, 2022 Cyber Security Survey



In October, 2022, Gartner released a report titled, “2023 Planning Guide for Identity and Access Management.” The key findings include:

- Identity and access management (IAM) is foundational to security, digitalization, cloud migration, remote work and operational efficiency. This places growing demands on IAM architecture and teams
- Identity-first security requires new architectural approaches to IAM and security in order to reduce security gaps and delays in detecting and responding to problems

The report highlights the business value of Identity Governance and Administration (IGA) solutions.

According to Gartner, IAM is foundational to modern distributed digital activities. Security and risk management technical professionals must evolve their IAM roadmaps and architecture to provide identity-first security, and improve usability and dynamic interoperability as part of their 2023 initiatives.

It also underscores the need to embrace holistic risk mitigation strategies that align continuous external vulnerability monitoring to internal access control monitoring as a fundamental way to protect information and meet compliance requirements.

The Current State of Privacy Laws in Australia

As governments, regulatory entities, and industry standards organisations and agencies look to enforce security through compliance, risks become financial drivers for many companies.

And because the threat landscape is constantly changing, the regulatory landscape must change to keep up. Recently, Australian authorities released several critical cybersecurity and privacy documents that support best practices and, in some cases, institute fines. Understanding the overarching requirements and how they relate to Identity Governance and Administration (IGA) can help organisational stakeholders mitigate the continued risks facing their business.

Australian Privacy Act

On January 1, 2019, the Australian legislature updated the Australian Privacy Act (APA). The APA is the hallmark piece of legislation regarding handling the personal information of individuals, including collection, use, storage, and disclosure. The revised APA incorporates several significant provisions changing how public and private entities must manage information.

First, the law applies to State or Territory authorities "as if the authority or instrumentality were an organisation." Thus, the law specifically applies to both public agencies and governments as well as private businesses.

Second, it establishes an extraterritorial reach by defining owners/operators as Australian citizens/companies/subsidiaries. This definition means that an Australian citizen owning or operating a business in another country must adhere to the law.

By applying to access rather than acquisition, the update to the Australian Privacy Act highlights the importance of identity and access governance as fundamental to maintaining data privacy.

Third, the revision focused on data "at risk" of unauthorised access or disclosure that would lead a reasonable person to assume likely harm.

The APA shifts privacy from "unauthorised acquisition" to "unauthorised access." One identity governance concern facing public and private entities is that access to an application may be authorised, but access to specific information within that application may not be appropriate.

According to the Australian Privacy Principles (APP Schedule 1), a regulated entity must:

- Define the kinds of personal information that the entity collects and holds
- Define the purposes for which the entity collects, holds, uses, and discloses personal information
- Not use or disclose the information for a different purpose than the ones defined
- Take reasonable steps to protect the information from misuse, interference, and loss and from unauthorised access, modification, or disclosure

Privacy regulations continue to be strengthened

More recently, the passing of the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, enhanced the Office of the Australian Information Commissioner's (OAIC) ability to regulate in line with community expectations and protect privacy in the digital environment.

The Bill introduces significantly increased penalties for serious and or repeated privacy breaches and greater powers for the OAIC to resolve breaches[1].

In addition, 2024 is expected to see new legislation which will include the right to opt out of data collection (and time limits to keeping personal data); the inclusion of small businesses in the Privacy Act; and a right to be forgotten.

These changes mean organisations need a flexible platform, and one which can adapt to their requirements as privacy laws continue to be updated.

Australian Government Information Security Manual

Updated and republished in March 2023, the Australian Information Security Manual (ISM) sets forth strategic guidance and cybersecurity principles across four key activities: governance, protection, detection, and response.

Specifically, compliance with the ISM requires using a risk-based approach to cybersecurity. Additionally, as regards identity and access governance, the ISM applies controls such as:

- Reviewing business requirements and verification of need to access systems, applications, and data repositories
- Limiting privileges to only those necessary to fulfill job function
- Revalidating access on an annual or more frequent basis
- Limiting privileged user activities so that they cannot read emails, browse the web, or obtain files via online services such as instant messaging or social media to minimise the risk of compromising the accounts
- Restricting emergency access and setting time-bound rules for access termination in these circumstances

[1] https://www.oaic.gov.au/newsroom/oaic-welcomes-passing-of-privacy-bill

Although logical and seemingly simple, most agencies and organisations struggle to meet these requirements as they shift mission-critical operations to the cloud. Complex, interconnected security hierarchies across on-premises, hybrid, and cloud-based applications often provide users with excess access that compromises data privacy and security.

Essential Eight Maturity Model

Although not strictly a regulatory requirement with non-compliance penalties, the Essential Eight model, updated in November 2023, is well-accepted guidance set out by the Australian Cyber Security Centre. The Essential Eight Maturity Model acts as a regulatory cybersecurity framework for agencies and a set of best practices for corporations[2].

The Essential Eight maps out three levels of security program maturity based on controls around the following:

- Application Control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication

As the company increases the number of controls and its ability to reduce cyber risk, the organisation's program moves from "Level Zero" (least mature) to "Level Three" (most mature).

As part of maturing the organisation's security program, organisations and agencies need to take into account the following IGA concerns:

[2] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Essential Eight Requirement	Maturity Level One	Maturity Level Two	Maturity Level Three
Application Control	Application control is implemented on all workstations to restrict the execution of executables to an approved set.	Application control is implemented on all servers to restrict the execution of executables to an approved set. Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application control bypasses.
Restrict administrative privileges	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and information is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Identity and Access Governance: The Privacy Convergence

Public and private entities that need to comply with these seemingly divergent requirements may feel overwhelmed. However, despite their different languages, they converge on a single theme: limit user access to sensitive data.

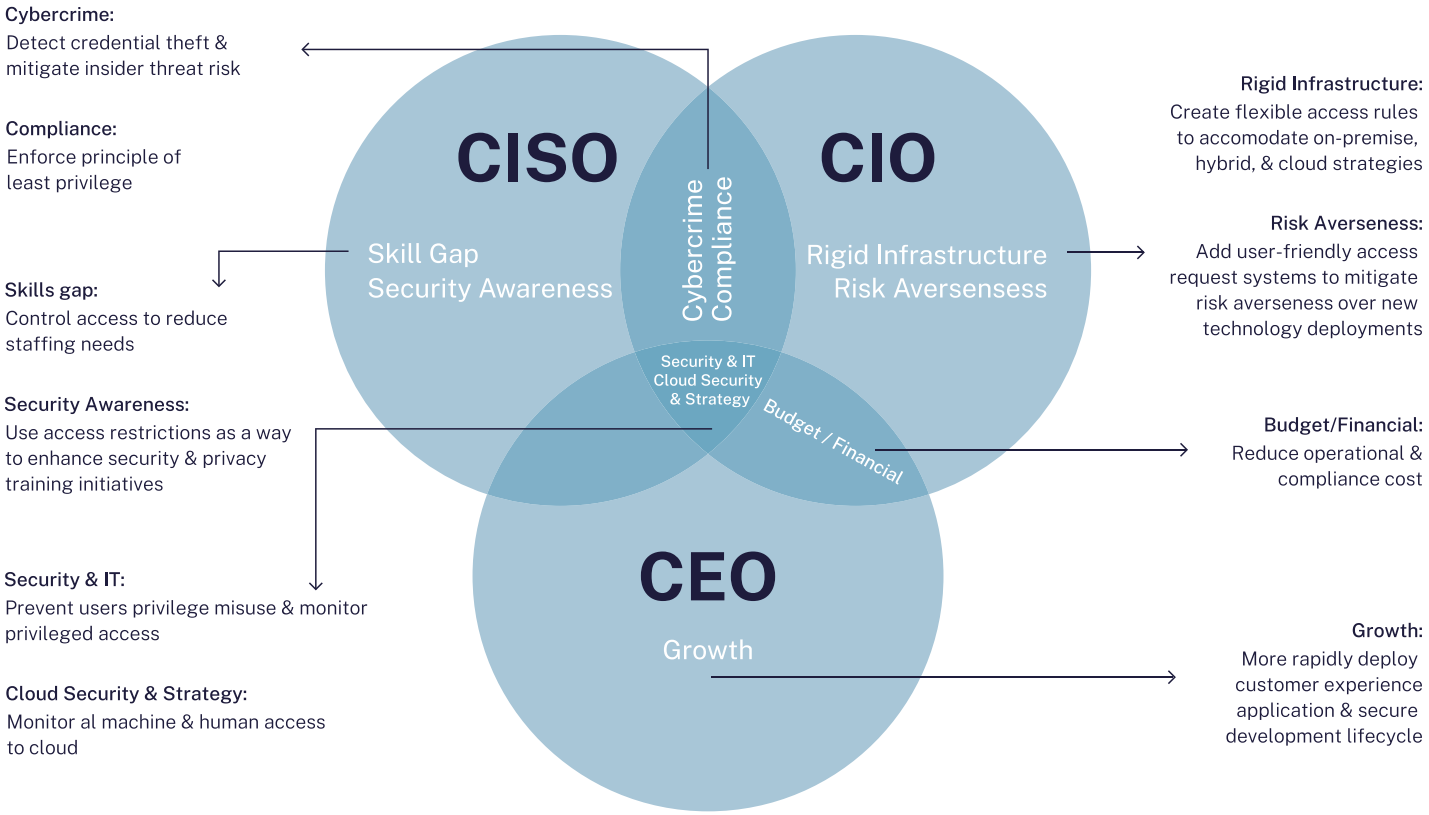
Many entities struggle with establishing and maintaining the principle of least privilege as they increase their digital footprint. According to Cloud and Threat Report 2024 by Netskope, cloud and SaaS adoption continued to rise in enterprise environments with the number of apps used by the average increasing from 14 to 20 over the past two years, an average 19 per cent increase per year. According to the report, half of all enterprise users interact with between 11 and 33 apps each month, with the top 1% of users interacting with more than 96 apps per month.

The report further points out over the past year, the percentage of malware downloads originating from SaaS apps has been consistently above 50 per cent, a trend that Netskope Threat Labs expects to continue through 2024.

To reduce those numbers to a single statement: maintaining compliance in today's complicated, increasingly cloud-based environment is difficult, time-consuming, and expensive.

Approaching Compliance Through an Identity-First Lens

Regardless of where an organisation is on its path to digital transformation and security maturity, approaching compliance through an identity-first lens provides several significant value-adds for all stakeholders.



Five Steps for Maturing and Modernising Data Privacy and Security

As organisations and government agencies transform their IT ecosystems with new technologies, they face unique struggles associated with controlling access to resources. It is even more frustrating for many companies; they need to monitor many identities, many of which they find difficult to control. Maintaining “least privilege” data access controls over customers and employees is only the first step.

The second step involves maintaining access controls over the alphabet soup of digital transformation, including but not limited to APIs, RPAs, IPAs, and IoT.

Analyse Risk

Nearly all compliance mandates begin with an annual risk analysis. However, as organisations and agencies add more cloud-based technologies to enable business operations, they need to focus on different risks.

As the organisation connects more applications and increases its cloud ecosystem complexity, these questions are no longer easy to answer. As users connect to cloud resources, ecosystem visibility continues to decrease while risk increases.

- Where is data located?
  - On-premises? Private cloud?
  - Public cloud? Hybrid ecosystem?
- What type of data is stored in each location?
- Who accesses data?
- Can the organisation limit access?
- Does the organisation apply broad or detailed access entitlements?
  - Can the organisation limit access within an application?
  - How does the organisation limit privileged access?
- Are time-bound limitations possible?

Determine Users

Determining users in legacy on-premises ecosystems was simple because organisations and agencies could better control access to resources. However, modernised ecosystems include new types of users, increasing enterprise privacy risk.

Organisations and agencies need detailed, segmented user identities that incorporate risk, moving beyond Role-Based Access Controls (RBAC). Best practices for governing access while managing privacy risk now require context-aware access controls aligned with Attribute-Based Access Controls (ABAC).

Some user types include:

- Employees
- Customers
- Service accounts
- RPA
- IPA
- IoT devices
- APIs

Set Controls

The first significant barrier enterprises face on their digital transformation journeys lies in setting appropriate access controls. Risk assessments are now more complex as identifying users becomes more time-consuming, yet organisations and agencies can still manage both of these steps. Setting controls, however, requires the ability to drill down into details such as applications, data, and location.

As part of this, organisations and agencies struggle to comply with segregation of duties (SOD) and manage non-digital account ownership succession. Relying on individual vendor-supplied identity and access management dashboards leaves organisations and agencies lacking a single location to review control effectiveness across all locations and identities.

To comply with data privacy mandates, organisations and agencies must review:

- Access points
- Applications
- Workloads
- Servers/Serverless
- Privileged Access
- Time-bound Access
- Request/Review/Certify Process
- Account/Identity Ownership
- Segregation of Duties (SOD)

Monitor Access

Anomalous access requests within the ecosystem create as much data privacy risk as unauthorised access from external malicious actors. Meanwhile, as users request additional access or as the enterprise adds new technologies, the number of access risks increases, leaving IT administrators overwhelmed.

IGA's history consists of niche products and homegrown solutions that no longer meet the needs of companies seeking digital transformation. Now, each cloud-based technology provides tools and definitions for monitoring identities, roles, and groups. Simultaneously, these products remain isolated, leading to a lack of visibility and increased human error risk.

As part of continuous monitoring, companies must be able to review access requests based on:

- Role-based Access
- Group-based Access
- Separation of Duties Violations
- Peer Access
- Usage-Based Access
- Time-bound Access
- Joiner/Mover/Leaver Access
- Privileged Access
- IoT/RPA/IPA/API Access
- Ownership Succession
- Orphaned Accounts

Document Decisions

All compliance mandates require governance over the organisation's data privacy and security programs. Unfortunately, with multiple technologies across the IT ecosystem, many organisations and agencies find that the onboarding process increases complexity. At the same time, their IT administrators become overwhelmed with the onslaught of requests that require review and certification.

To document access decisions, organisations and agencies need to:

- Determine Account Ownership
- Manage Succession
- Review Access Requests
- Engage in Compliance Required Access Reviews

Managing documentation through written requests or IT ticketing systems is a time-consuming process that increases operational costs and human risk. To enable business operations as the influx of requests and reviews becomes overwhelming, IT departments and managers approve all access – traditionally called "rubber stamping." This process lacks the necessary documentation, leaving organisations and agencies suffering from audit findings.

Intelligent Compliance-as-a-Service with Saviynt

Saviynt Identity Cloud delivers flexible on-premises or cloud deployments, and automates these compliance steps using peer and usage-based analytics. The Identity Cloud combines multiple identity management capabilities (identity governance, privileged access, third-party access, and application & data access governance) into a single cohesive platform – unifying controls, analytics, and risk management for every identity, app, and cloud across your business.

Saviynt's intelligent identity analytics modernise IGA by providing predictive access, enabling organisations and agencies to set the complex, adaptive, risk-aware policies necessary for proving governance across interconnected ecosystems.

Reconcile Roles for a Standardized Authoritative Identity Source

Saviynt's identity warehouse imports the identity definitions from across all on-premises and cloud-based resources to create a single authoritative source for identity. Using built-in role-mining capabilities, administrators can review the definitions that each resource uses, locate the commonalities, and obtain suggested authoritative definitions. They can choose to use human resource management systems, another application or cloud-based resource, or Saviynt's platform as the authoritative source of identity.

Automate Requests, Reviews & Certification to Continuously Monitor Controls

Our analytics streamline the request/review/certify process by suggesting additional access to enable users or alerting the organisation to potential SOD violations. Our peer and usage-based analytics compare how users interact with data across the organisation to automate the process. When users request access, the analytics compare that user's data to others with the same attributes – and can automatically provide the access if the two match. However, if the user's request is anomalous, Saviynt's platform elevates the request for additional review. If the request poses an SOD violation, AI and machine learning suggests a remediation action.

Manage Machine Identities for Holistic Access Governance

Moreover, Saviynt's platform enables organisations and agencies to assign non-human user identities. For example, an RPA can be assigned an identity within the platform, and then the organisation can assign an owner responsible for monitoring the activity.

Administrators can also assign a line of succession so that if the original responsible owner is no longer available, the RPA or other non-person identity will still be assigned a reviewer. By assigning these responsibilities in the system, the organisation maintains continuous governance over these elusive identities.

Protect Sensitive & Privileged Access with PAM

Rather than needing to use two services - one for IGA and one for PAM - Saviynt's PAM solution brings the two together in a single solution to ease audit and lifecycle management. Saviynt PAM plus IGA uses intelligent analytics to streamline the request/review/certify process establishing full governance of both policy and access, removing the bloat of unneeded groups, offering clear audit of administrative activity, and removing the risk of human error. Using Saviynt's solution, administrators request and access their terminal sessions within our browser-based interface. Once approved, the administrator can launch the session directly within the browser, solving the problems and risks associated with downloading SSH clients or connecting through jump hosts. All activity through the sessions can be monitored and is recorded.

By converging IGA and PAM capabilities into one solution, PAM enables organisations and agencies to review, request, and certify privileged access using context and risk.

ABOUT SAVIYNT

Saviynt's Identity Cloud helps modern enterprises scale cloud initiatives and solve the toughest security and compliance challenges in record time. The company brings together identity governance (IGA), granular application access, cloud security, and privileged access management (PAM) to secure the entire business ecosystem and provide a frictionless user experience. The world's largest brands trust Saviynt to accelerate business transformation, empower distributed workforces, and meet continuous compliance, including BP, Western Digital, MassMutual, Koch Industries. For more information, please visit **www.saviynt.com**.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suit e D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com