SAVIYNT

Cloud Access Governance & Intelligence

for Data, Infrastructure & Applications

IDENTITY IS THE NEW PERIMETER

IT is undergoing a huge transformation as enterprises increasingly adopt the Cloud to meet business demands for elasticity, flexibility, and scalability. With hybrid IT becoming a norm, critical enterprise assets are now distributed: sensitive data or critical infrastructure already resides on the Cloud and outside the enterprise's traditional perimeter.

The responsibility for appropriate and consistent enforcement of compliance and security controls and policies lies with the enterprise. With each cloud provider offering varying degrees of control over security, identity has become the common thread that binds the security and trust fabric together.

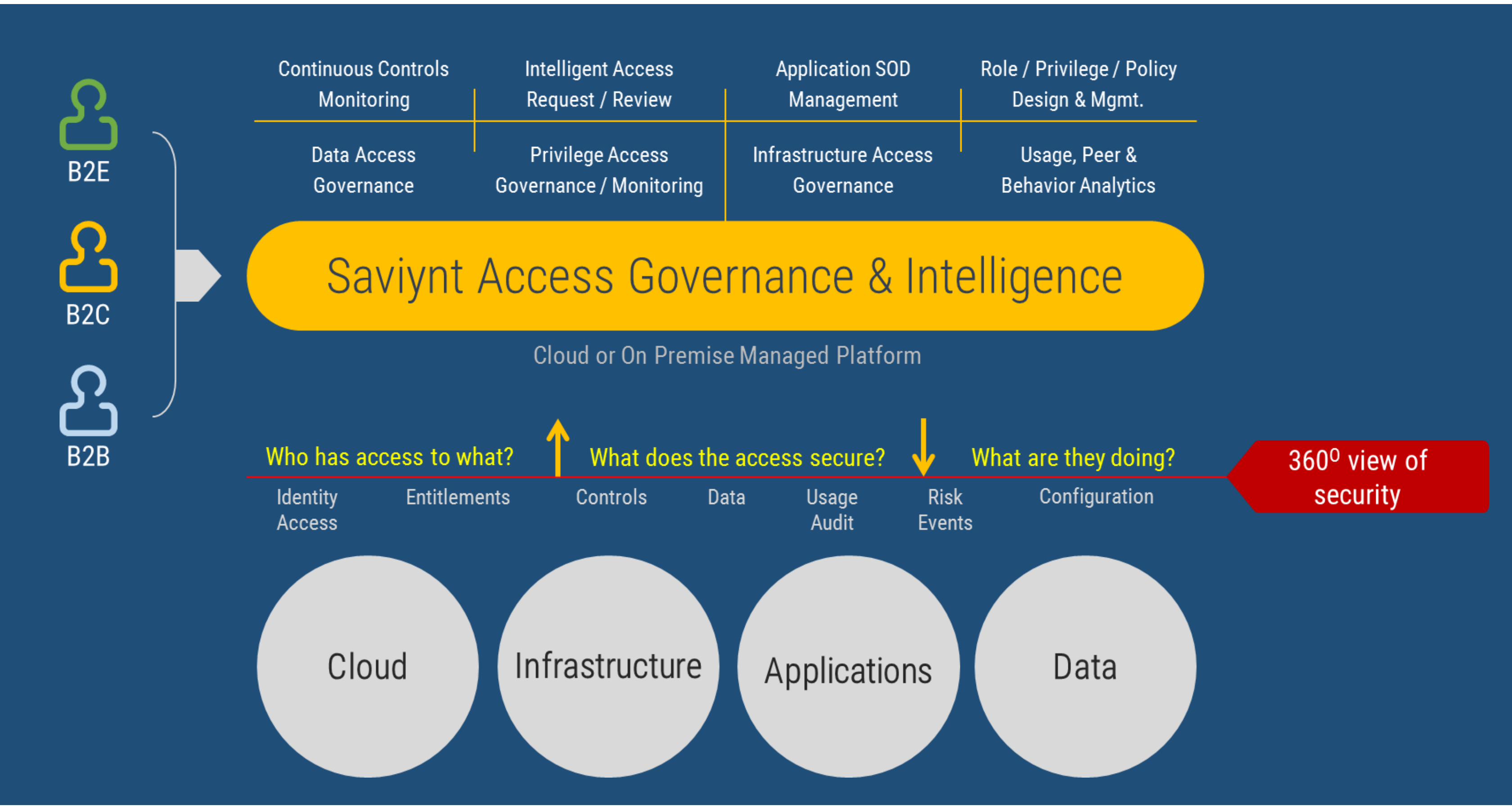
RISK-BASED IDENTITY MANAGEMENT IS THE KEY TO SUCCESS

Identity Governance and Administration (IGA) tools have typically been driven by compliance and automation needs and do not account for large volume and types of identities such as users, devices, business partners, customers, etc. In addition, most IGA tools only understand coarse-grained access and cannot be easily extended to secure data, infrastructure, and fine-grained application entitlements.

A sustainable way to implement IGA across Cloud and enterprise in an efficient and effective manner is to take a risk-based approach. Risk is key to determining who has access to critical business functions, PHI/PCI/SOX data, or sensitive/vulnerable workloads. This allows a finite amount of IGA resources to be effectively deployed to secure risky users and risky access.

INTRODUCING SAVIYNT CLOUD ACCESS GOVERNANCE AND INTELLIGENCE

Saviynt delivers the next generation of IGA 2.0 that provides a single pane of glass of users' access across data, infrastructure, and applications that reside on the Cloud or enterprise. Saviynt's Cloud Access Governance and Intelligence platform, delivered either from the Cloud or on-premise, combines intelligent IGA processes with usage and risk analytics.



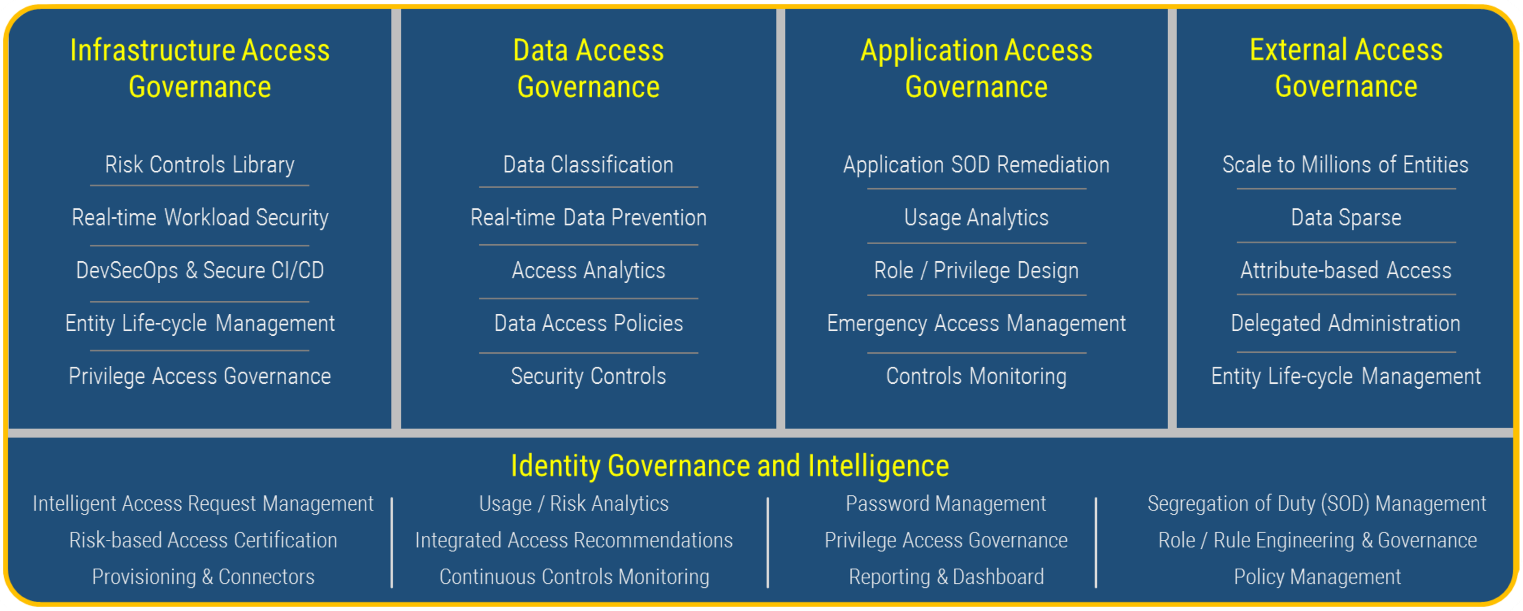
B2E
B2C
B2B
Continuous Controls Monitoring
Intelligent Access Request / Review
Application SOD Management
Role / Privilege / Policy Design & Mgmt.
Data Access Governance
Privilege Access Governance / Monitoring
Infrastructure Access Governance
Usage, Peer & Behavior Analytics
Saviynt Access Governance & Intelligence
Cloud or On Premise Managed Platform
Who has access to what?
What does the access secure?
What are they doing?
360⁰ view of security
Identity Access
Entitlements
Controls
Data
Usage Audit
Risk Events
Configuration
Cloud
Infrastructure
Applications
Data

- Who has access to what – implementing purpose-built deep integration connectors for Cloud and enterprise applications/platforms

- What does the access secure – identifying what type of data (e.g., PCI, PHI, financial, and sensitive), business functions, and/or infrastructure does the user have access to and what can they perform with that access (e.g., modify, read-only, and delete)

- What are they doing with their access – collating and analyzing usage and audit logs from managed platforms, log aggregators, etc.

Saviynt enables enterprises to enforce intelligent and risk-based IGA processes with a modular architecture for securing data, infrastructure and application access for internal and external users.



Infrastructure Access Governance	Data Access Governance	Application Access Governance	External Access Governance
Risk Controls Library	Data Classification	Application SOD Remediation	Scale to Millions of Entities
Real-time Workload Security	Real-time Data Prevention	Usage Analytics	Data Sparse
DevSecOps & Secure CI/CD	Access Analytics	Role / Privilege Design	Attribute-based Access
Entity Life-cycle Management	Data Access Policies	Emergency Access Management	Delegated Administration
Privilege Access Governance	Security Controls	Controls Monitoring	Entity Life-cycle Management

Identity Governance and Intelligence

Intelligent Access Request Management	Usage / Risk Analytics	Password Management	Segregation of Duty (SOD) Management
Risk-based Access Certification	Integrated Access Recommendations	Privilege Access Governance	Role / Rule Engineering & Governance
Provisioning & Connectors	Continuous Controls Monitoring	Reporting & Dashboard	Policy Management

SAVIYNT IDENTITY GOVERNANCE IS INTELLIGENT

The core Saviynt IGA platform incorporates several unique risk and usage analytics features such as:

- Integrated access recommendations – derived from the inlier analysis of user's access as compared to peers. These recommendations are made available to the requester as 'people like you have access to' while shopping for access.

- Usage/activity-based risk decisions – arrived at by analyzing users' usage reports (i.e., indicating how often, when, and how the entitlement was used). This decision is then provided to certifiers during access attestation/certification process to make an informed decision.

- Policy-based risk decisions – analyzed by combining entitlement criticality, access outlier analysis, potential violation of business policies, and/or segregation of duty (SOD) rules. These decisions are included when requests are dynamically routed to approvers to understand the impact if access is approved.

SAVIYNT

SAVIYNT INFRASTUCTURE ACCESS GOVERNANCE

Organizations are rapidly migrating workloads (including critical ones) from traditional data centers to IaaS providers, such as AWS and Azure. In addition, they are adopting SDLC processes, such as DevOps and Continuous Integration/Continuous Delivery (CI/CD).

CHALLENGES

1 High risk due to privileged access…

Compromise of a single AWS / Azure Account can lead to breach of entire virtual datacenter on Cloud

DevOps users can have privileged access to IaaS services / workloads / policies and CI/CD tools in their VPCs

2 Complex services and entities to manage…

Access control extends beyond users to entities such as VPCs, subnets, instances, DBs, data objects, etc. Policies are usually defined as JSON objects

Multiple points of risk such as incorrect workload tags, misconfigured instances, open ports / open access, non-rotated certificates, etc.

Need to keep pace with IaaS innovation e.g. Amazon released 200+ capabilities and services for AWS in 2015 alone

3 Scale and intelligence is a must…

Visibility of a single AWS account needs integration with at least 5 log sources including CloudWatch, CloudTrail, VPC flow logs, AWS Config, several DevOps tools, etc.

Large volumes of user access, configuration and activity data need smarter tools such as intelligence and analytics to identify riskiest users and access

SOLUTION

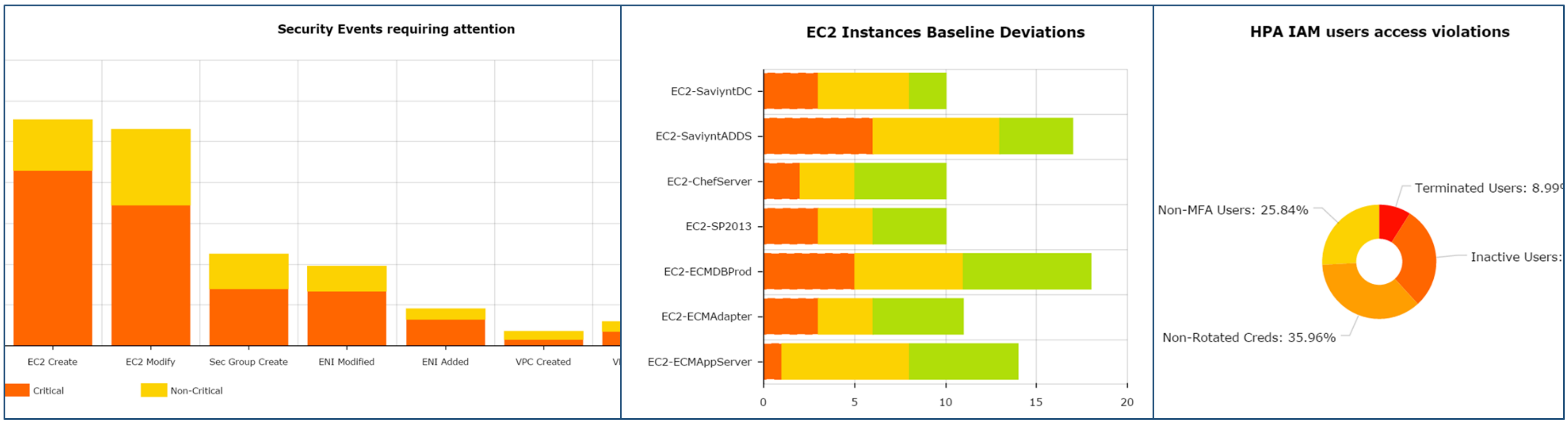
SAVIYNT INFRASTRUCTURE ACCESS GOVERNANCE

- Out of box controls library with 70+ risk signatures and actionable controls
- Real-time prevention of risky actions e.g. launch of workloads that violate security policies, unauthorized access escalations or role modification, etc.
- Privilege access governance
- Adoption of DevSecOps & secure CI/CD
- Comprehensive entity life-cycle management integrated to enterprise authoritative sources

amazon web services™ GitHub CHEF™

Windows Azure puppet labs

DASHBOARD



REAL-TIME PREVENTIVE POLICIES

Non BootStrapped Instances	**If** Infrastructure.Instance Type **EQUALS** "Production" **AND** Infrastructure.Bootstrap Status **EQUALS** "0" . **AND** "Notify Manager"
Default Sec Group	**If** Infrastructure.Security Group **IS** "default" . **AND** "Terminate"

SAVIYNT DATA ACCESS GOVERNANCE

According to a recent survey, Microsoft Office 365 is one of the most widely adopted Cloud applications. Along with numerous productivity and collaboration benefits, such adoption has the potential for loss of sensitive information if the appropriate security is not implemented.

CHALLENGES

1 Access model is discretionary (DAC)…

A user with read-only access to a sensitive document can share it with any internal user (or external)

Access escalation or privilege modification performed by Privileged User can go unnoticed

2 Files can be exchanged without 'sharing'…

A user can create 'share link' for a document and distribute it out-of-band leaving no trace and open to anonymous access

3 Data encryption is not enough…

It protects only against external rogue access or if service provider is compromised. Authorized users with appropriate access still get access to encrypted data

Gateway-based encryption strategies might not work well with mobile access

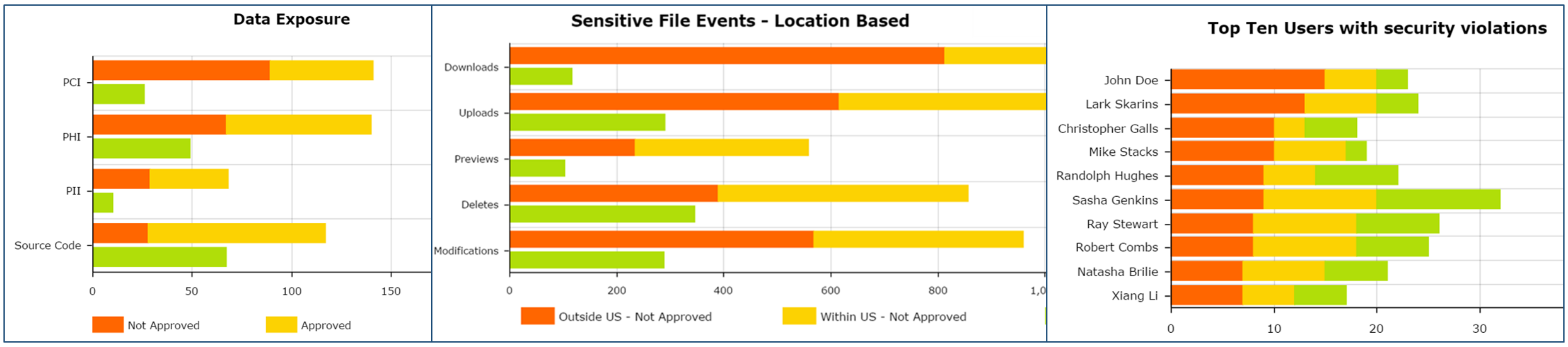
SOLUTION

SAVIYNT DATA ACCESS GOVERNANCE

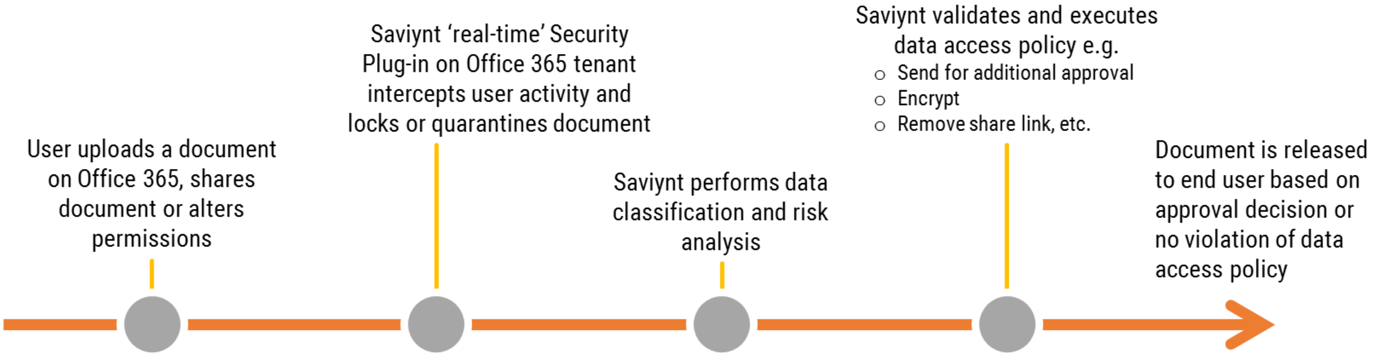
- Data classification with 50+ signatures
- Real-time data prevention including quarantine, approval, revoke share, etc.
- Integrated access hierarchy analysis and user behavior analytics
- Data access policies
- Privilege access governance
- Access life-cycle management
- On-tenant API-based security plug-in for consistent policy enforcement across web and mobile

Office box Google Apps for Work SharePoint Dropbox

DASHBOARDS



REAL-TIME PREVENTIVE POLICIES



User uploads a document on Office 365, shares document or alters permissions

Saviynt 'real-time' Security Plug-in on Office 365 tenant intercepts user activity and locks or quarantines document

Saviynt performs data classification and risk analysis

Saviynt validates and executes data access policy e.g.
- Send for additional approval
- Encrypt
- Remove share link, etc.

Document is released to end user based on approval decision or no violation of data access policy

SAVIYNT APPLICATION ACCESS GOVERNANCE

Saviynt assists enterprises to meet compliance mandates by offering one of the most advanced SOD management solutions while including features, such as a controls library, risk-based access certification, and emergency access management. The platform enables internal audit and security teams to define business rules, identify conflicts/violations, monitor critical transactions, remediate violations, and assess their impact via an intuitive SOD management workbench.

With its ability to understand complex entitlement hierarchy independent to each application, Saviynt's solution can perform enterprise-wide cross application SOD analysis. In addition, Saviynt integrates usage analytics to identify actual SOD violations that have been acted upon by users vs. potential SOD violations and helps prioritize remediation measures.

CHALLENGES

1 Most are mission critical…

Strict access control especially for privileged access is a must to secure mission critical data and transactions

Ever increasing compliance mandates dictate deployment and continuous monitoring of GRC and security controls

2 Authorization is complex, hierarchical & unique…

Each application has potentially multiple modules with varied architecture, unique and complex access hierarchy implementation

Segregation of duty (SOD) enforcement / fraud management is complex, needs automation and deep integration with application's access hierarchy

3 Typically managed in a silo…

Enterprise applications have a standalone security solution, leading to inconsistencies and redundancy in policy enforcement

SOLUTION

SAVIYNT APPLICATION ACCESS GOVERNANCE

- Application SOD management & remediation
- Mitigating controls management
- Usage and risk analytics
- Access recommendations
- Role / privilege design & governance
- Emergency access / firefighter management
- Security controls library with actionable controls

salesforce

ORACLE E-BUSINESS SUITE

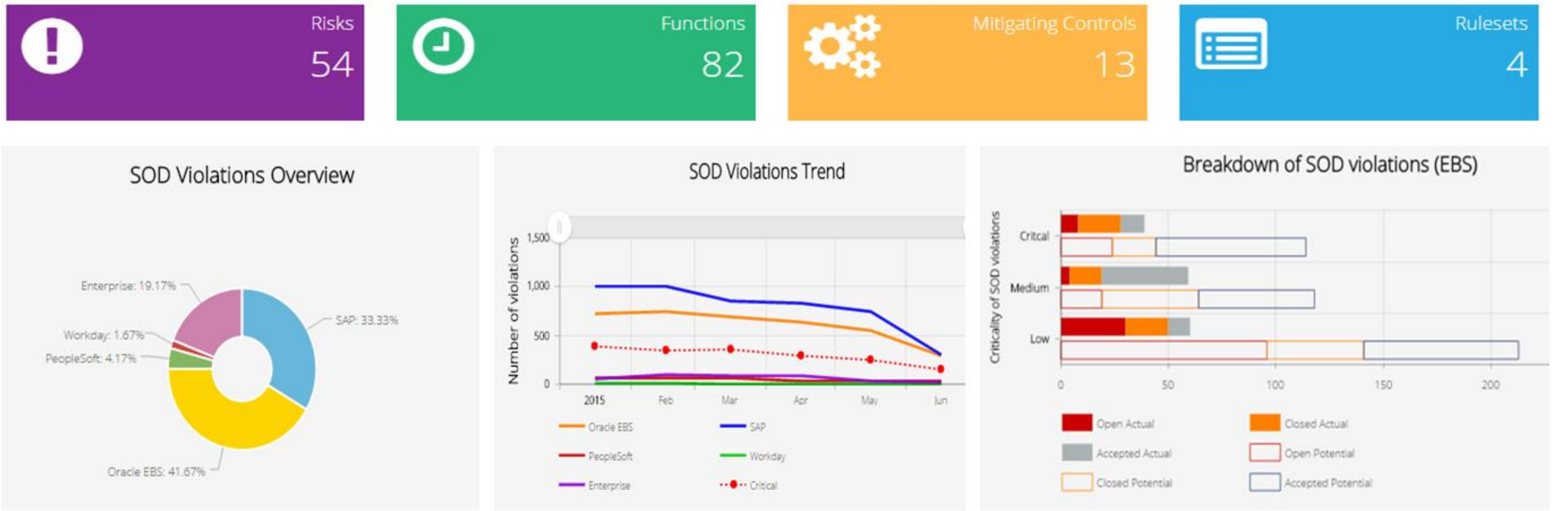
SAP HANA

Epic

SAP

PeopleSoft

DASHBOARDS



SAVIYNT EXTERNAL ACCESS GOVERNANCE

As enterprises collaborate with multiple business partners to thrive, they often struggle to find the right balance between exposing their internal systems and enforcing security. In most cases, IGA tools do not support the appropriate granularity or scale needed for controlled delegation of millions of users' administration to partners.

CHALLENGES

1 Need to support Digitization initiatives…

Involves empowering customers and partners with self-service tools and opening up traditionally closed IT processes

Requires support for multiple types of access channels such as IOT, analyzing customer behavioral intelligence, etc.

2 Security must scale to millions of entities…

Solution needs to provide granular access control over services, attributes and fields

Such scale requires IDM solution to be data sparse and support fine-grained delegated administration and profile management

3 IDM integration needs to run deep…

Needs to support extensive APIs and flexible configuration to seamlessly integrate with rest of customer experience

SOLUTION

SAVIYNT EXTERNAL ACCESS GOVERNANCE

- Proven to scale for millions of entities
- Inherent support for data sparse model
- Granular attribute-based access control (ABAC)
- Self-service and delegated administration
- Entity life-cycle management
- Attribute and permission inheritance
- Federation support
- Group provisioning

salesforce okta FORGEROCK OpenDJ Azure AD RADIANT LOGIC

EMBRACE CLOUD-FIRST STRATEGY WITH CONFIDENCE

In today's age of hybrid IT, identity is central to securing critical assets on Cloud and Enterprise. Saviynt's Cloud Access Governance and Intelligence solution is:

- Built for Cloud
- Intelligent and risk-driven
- Unified solution for securing applications, data and infrastructure
- Scalable to millions of identities
- Managed platform that continuously evolves to changing needs

ABOUT SAVIYNT

Saviynt is a leading provider of next generation Identity Governance and Administration solutions for Data, Infrastructure and Critical Applications for the Cloud and Enterprise. Saviynt combines traditional IGA features with advanced usage analytics, data/infrastructure access governance, user behavior analytics, real-time threat detection, and compliance controls to secure organization's critical assets.

CORPORATE HEADQUARTERS

5777 W Century Blvd, Suite 360
Los Angeles 90045
info@saviynt.com
+1 (314) 641-1664
www.saviynt.com