SecurEnds Product Portfolio

Overview

We **enable CISOs and CIOs to transform their organization's compliance posture, reducing cyber risk**, while making teams more efficient.

SecurEnds **UAR (User Access Reviews)**

SecurEnds **SoD (Separation Of Duty)**

SecurEnds **AR (Access Request)**

SecurEnds GRC **(Governance Risk & Compliance)**

Our powerful SaaS platform purpose-built to automate user access reviews, eliminate dormant and risky accounts, and uphold segregation of duties (SoD) controls. Our Access Request module speeds up onboarding while maintaining governance, and our **T-Hub gateway** enables seamless, standards-based provisioning across hybrid environments. With advanced identity analytics, comprehensive audit readiness, and out-of-the-box connectors, SecurEnds helps organizations accelerate compliance, improve security posture, and reduce administrative overhead—all with a rapid time-to-value

10

Compliance Standards

SOX, SOC, PCI, ISO, HIPAA, FFIEC, GDPR, CCPA, GLBA, FDA 21 CFR

150+

Global Customers

USA, India, Japan, Mexico, Belgium, Australia, Netherlands

Recognized By

Deloitte. KuppingerCole ANALYSTS Gartner

ALCHEMY Insight shi pwc

Market Recognition

incomm payments

TowneBank

loanDepot

INDEPENDENT FINANCIAL

FARMERS & MERCHANTS STATE BANK

First United Bank & Trust

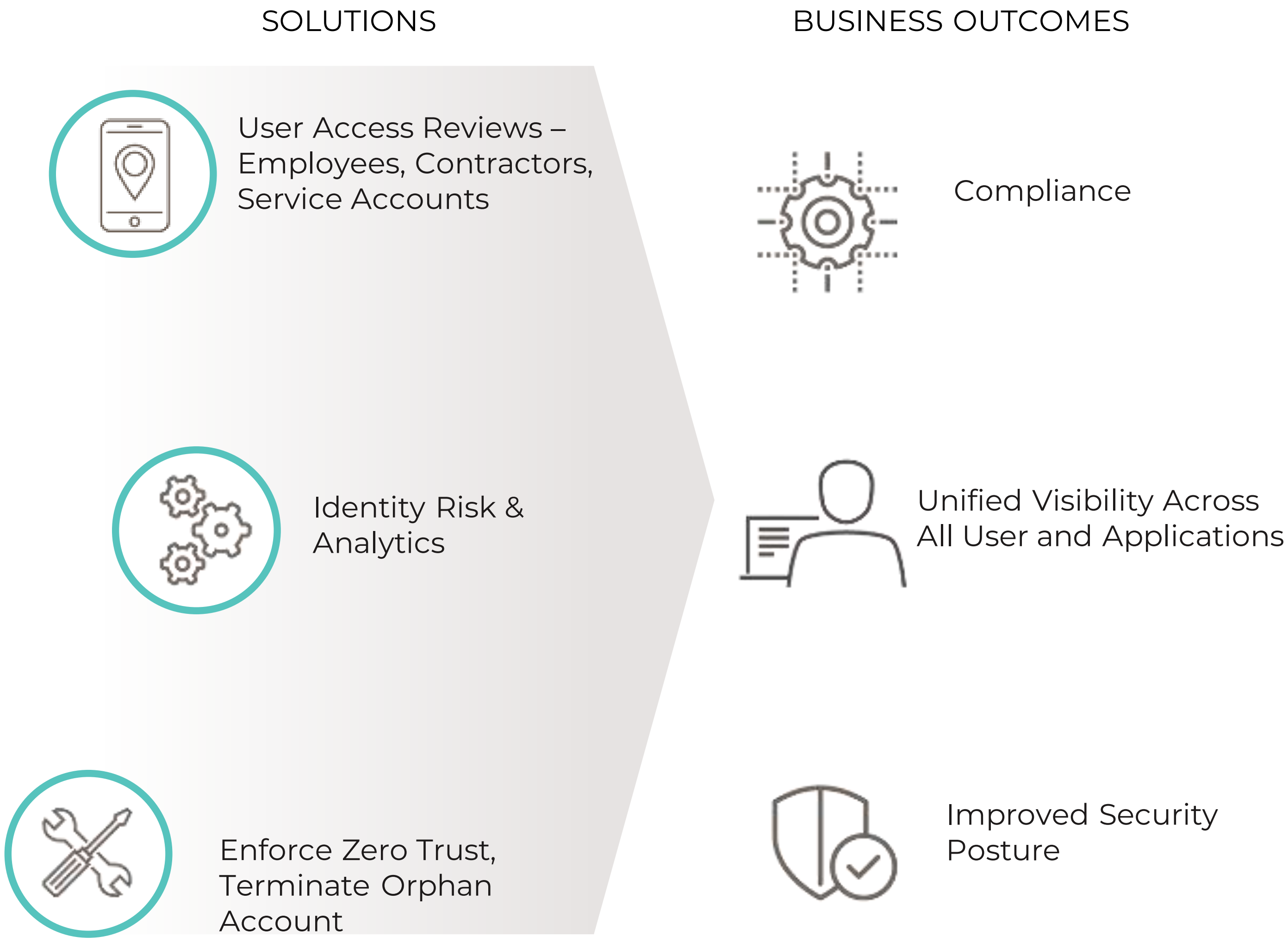
CAPTRUST

COMPEER FINANCIAL

summit CREDIT UNION

REPUBLIC BANK & TRUST

AMG National Trust



SOLUTIONS

User Access Reviews – Employees, Contractors, Service Accounts

Identity Risk & Analytics

Enforce Zero Trust, Terminate Orphan Account

BUSINESS OUTCOMES

Compliance

Unified Visibility Across All User and Applications

Improved Security Posture

SecurEnds IGA Modules

User Access Review

User Access Review module provides organizations with an automated solution to review, certify, and audit user entitlements across applications, systems, and data sources—ensuring compliance, reducing access risk, and maintaining least-privilege principles.

Access Request

The SecurEnds Access Request module provides organizations with a streamlined solution to manage, route, and fulfill user access requests—enabling faster onboarding, enforcing approval workflows, and maintaining governance over access assignments.

SoD

The SecurEnds Segregation of Duties (SoD) module provides organizations with a proactive solution to detect, prevent, and remediate conflicting access rights—safeguarding critical systems against fraud, operational errors, and compliance violations.

Identity Analytics

The SecurEnds Identity Analytics module provides organizations with deep insights into user access patterns, role anomalies, and entitlement risks—empowering data-driven decisions to optimize access controls, enforce least privilege, and strengthen security posture

T-Hub

The SecurEnds T-Hub module provides organizations with a flexible, standards-based integration gateway that facilitates seamless identity provisioning and deprovisioning across diverse IT environments. Built on SCIM and REST APIs, T-Hub enables bi-directional data flow between SecurEnds and various systems, including Active Directory, Azure, Okta, and custom applications. This middleware API gateway streamlines identity governance processes, reduces manual interventions, and accelerates onboarding and offboarding workflows

User Access Reviews

Human Identity

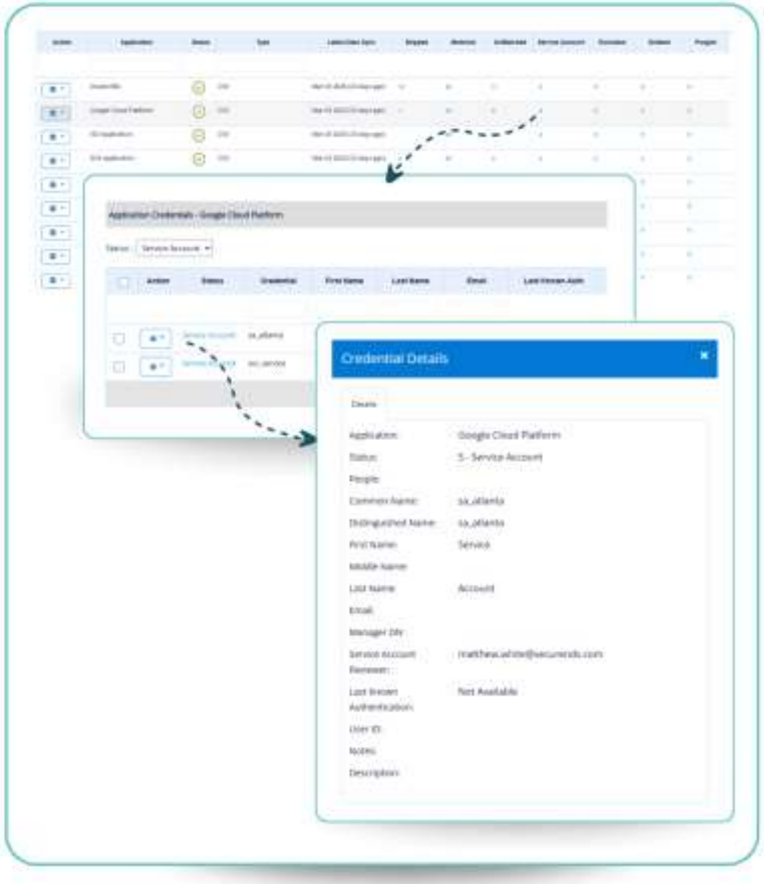
SecurEnds enables managers, entitlement owners, and application owners to conduct both single and hierarchical access reviews for employees, vendors, and contractors. Organizations can aggregate identity data from multiple applications into a unified system of record, leveraging fuzzy logic to intelligently associate usernames and credentials across different platforms. This ensures a comprehensive and accurate identity review process.

Non-Human Identity

SecurEnds Non-Human Identity Management streamlines the governance of service accounts, ensuring they are properly classified, reviewed, and assigned to responsible owners. Organizations can manually assign service accounts via the UI or use bulk assignment for efficiency. Service accounts are automatically included in access reviews, ensuring continuous monitoring and compliance.

Entitlement Management

SecurEnds enables entitlement management by continuously refining access policies, enforcing least-privilege principles, and eliminating security gaps. With SecurEnds, organizations can identify and remediate over-privileged users, orphaned accounts, and excessive entitlements, ensuring that future access requests align with business needs and security best practices. By dynamically adjusting entitlement policies, organizations can prevent privilege creep, reduce security risks, and maintain compliance with evolving regulatory requirements.



Application Credentials - Google Cloud Platform

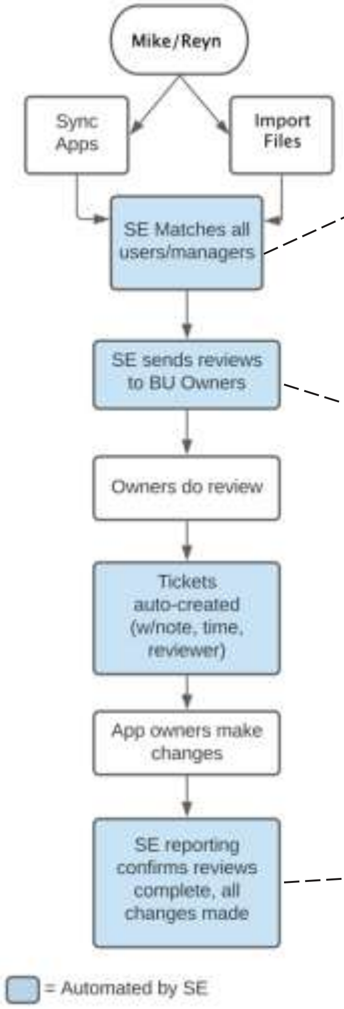
Credential Details

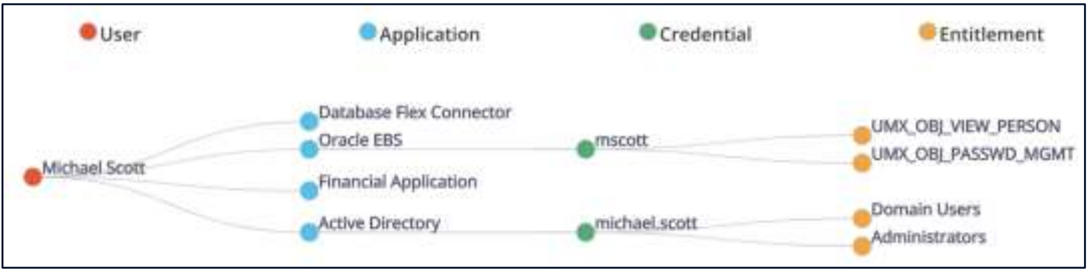
Details

Application:	Google Cloud Platform
Status:	S - Service Account
People:	
Common Name:	sa_atlanta
Distinguished Name:	sa_atlanta
First Name:	Service
Middle Name:	
Last Name:	Account
Email:	
Manager DN:	
Service Account Reviewer:	matthew.white@securends.com
Last Known Authentication:	Not Available
User ID:	
Notes:	
Description:	

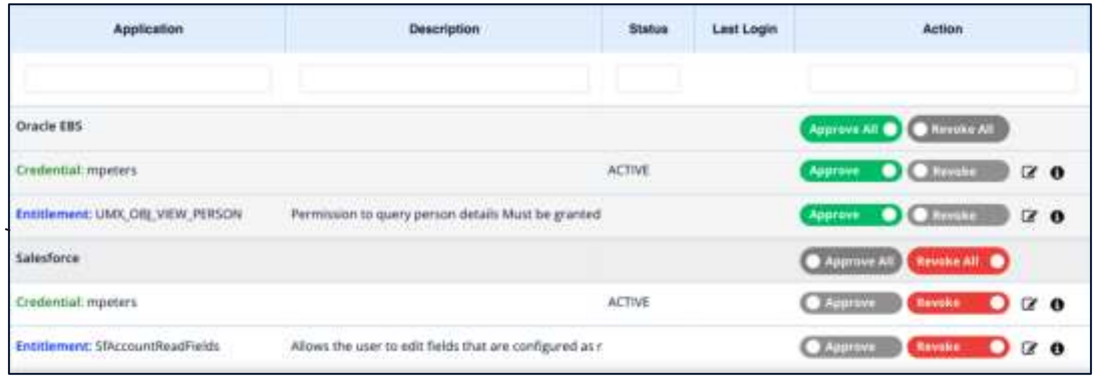
User Access Reviews

With SecurEnds


Mike/Reyn
Sync Apps
Import Files
SE Matches all users/managers
SE sends reviews to BU Owners
Owners do review
Tickets auto-created (w/note, time, reviewer)
App owners make changes
SE reporting confirms reviews complete, all changes made
= Automated by SE

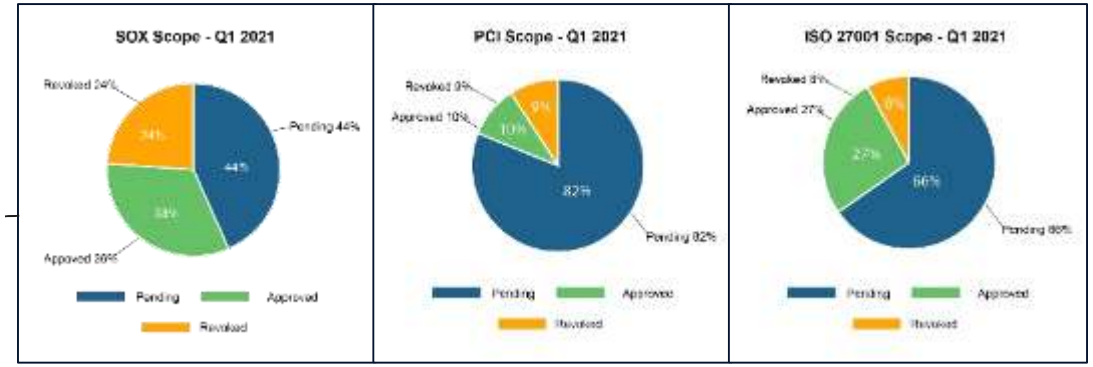


Visibility - "Who has access to what"



Application	Description	Status	Last Login	Action
Oracle EBS				Approve All ● ● Revoke All
Credential: mpeters		ACTIVE		Approve ● ● Revoke
Entitlement: UMX_OBJ_VIEW_PERSON	Permission to query person details Must be granted			Approve ● ● Revoke
Salesforce				● Approve All Revoke All ●
Credential: mpeters		ACTIVE		● Approve Revoke ●
Entitlement: SfAccountReadFields	Allows the user to edit fields that are configured as r			● Approve Revoke ●

User friendly access reviews

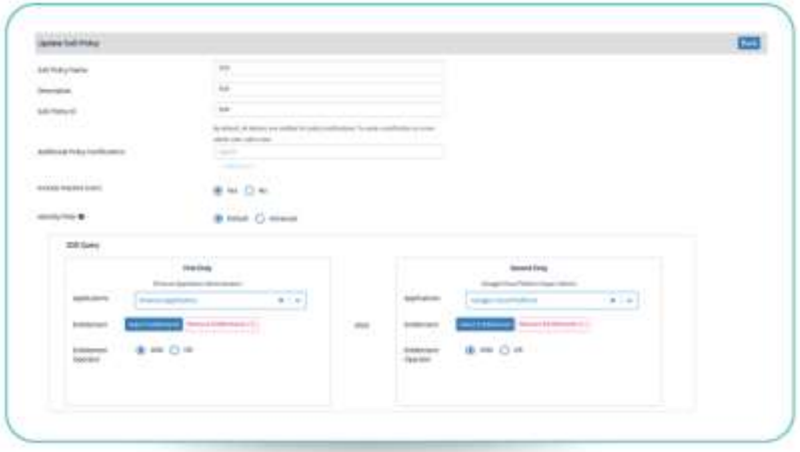


Compliance reporting

Segregation Of Duty (SoD)

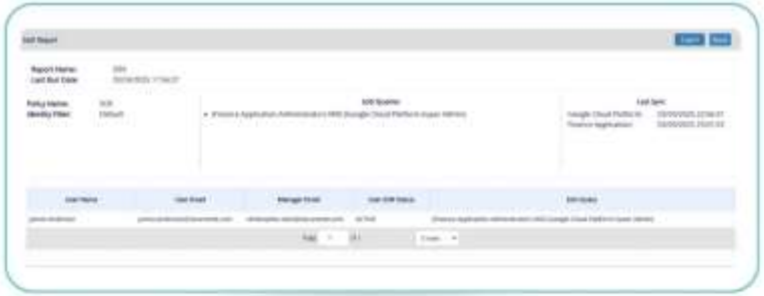
SoD Policy Builder

Ensure compliance and mitigate risk with SoD Policy Builder, enabling organizations to define and enforce Separation of Duties (SoD) policies across multiple applications. Administrators can create granular policies to prevent conflicts in access, such as restricting users from holding conflicting entitlements across different systems. With intuitive query-based configuration, organizations can easily enforce security best practices and reduce unauthorized access risks.



SoD Violation Reporting

Gain real-time visibility into policy violations with SoD Violation Reporting. This feature provides automated reporting on users who breach defined SoD policies, helping organizations quickly detect access conflicts that could lead to security threats. Reports can be scheduled daily, weekly, or monthly and exported in PDF format for audit and compliance tracking. Admins and designated recipients receive email notifications with detailed reports for proactive resolution.



Automated SoD Compliance Alerts

Stay ahead of security risks with Automated SoD Compliance Alerts. This feature ensures that administrators and designated stakeholders receive instant notifications whenever a policy violation occurs. The system automatically sends email alerts with attached reports, ensuring that violations are addressed promptly. By automating compliance monitoring, organizations can strengthen access governance and reduce the risk of fraud or insider threats.

Identity Analytics

Identity MindMap

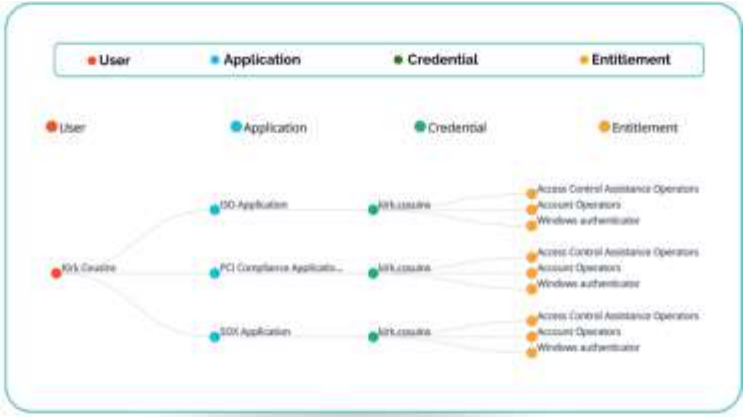
SecurEnds Identity MindMap Layout provides a user-centric view of access across applications and entitlements. It enables organizations to track a single user and identify orphaned accounts or access that exists outside the regular review cycle. This helps streamline deprovisioning, reduce security risks, and ensure only the necessary access is retained.

Application MindMap

SecurEnds Application MindMap Layout offers an application-centric perspective, displaying all associated users, credentials, and entitlements in a structured format. This view helps organizations identify and mitigate privilege creep, ensuring that users do not accumulate excessive access over time, thereby strengthening security and compliance efforts.

Entitlement MindMap

SecurEnds Entitlement MindMap Layout delivers an entitlement-centric view, mapping entitlements across applications and credentials. It is particularly useful for reviewing high-risk entitlements, such as administrative or privileged access, ensuring that critical permissions are properly assigned and regularly reviewed to prevent unauthorized access.



Users Report

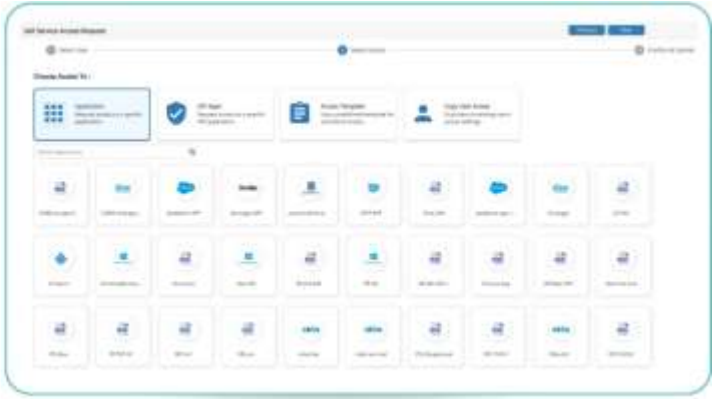
This report displays all users in the SOR and the list of applications that each user has access to.

Actions	First Name	Last Name	Employee Email ID	Employee Type	User Status in SOR	SOR Last Sync Date	Applications
⚙ ▾	Aaron	archer	[illegible]	Regular	Active		[illegible]
⚙ ▾	Aaron	archer	[illegible]	Regular	Active	[illegible]	[illegible]
⚙ ▾	Aaron	archer	[illegible]	Regular	Active		[illegible]
⚙ ▾	Aaron	[illegible]	[illegible]	Regular	Active	[illegible]	[illegible]
⚙ ▾	Aaron	[illegible]	[illegible]	Regular	Active	[illegible]	[illegible]
⚙ ▾	Aaron	[illegible]	[illegible]	Regular	Active		Active Directory
⚙ ▾	Aaron	[illegible]	[illegible]	Regular	Active		[illegible]

Access Request

Standard Self Service Access Request

SecurEnds Access Request Management streamlines the process of requesting and granting access across the organization. Users can select from three access types: Application Access, allowing direct requests for specific applications; Access Templates, enabling streamlined, role-based provisioning through pre-defined templates. Additionally, SecurEnds provides users with a centralized dashboard to track the progress of their access requests in real time allowing users to gain full transparency into the approval and fulfillment process, ensuring they stay informed at every stage.

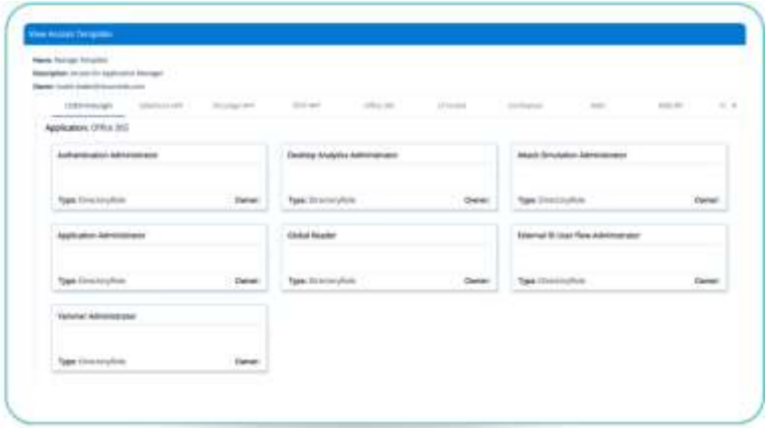


Self Service Access Request

Choose Access To :

Just-in-Time (JIT) Access

SecurEnds Just-in-Time (JIT) Access enhances security and compliance by granting users temporary, time-bound access to critical applications and resources only when needed. By eliminating standing privileges, JIT access reduces the attack surface, minimizes privilege creep, and enforces least privilege principles. Users can request access dynamically, ensuring that permissions are granted only for a defined duration before being automatically revoked.



View Access Template

Application: Office 365

Authentication Administrator
Type: DirectoryRole Owner:

Desktop Analytics Administrator
Type: DirectoryRole Owner:

Attack Simulation Administrator
Type: DirectoryRole Owner:

Application Administrator
Type: DirectoryRole Owner:

Global Reader
Type: DirectoryRole Owner:

External ID User Flow Administrator
Type: DirectoryRole Owner:

Yammer Administrator
Type: DirectoryRole Owner:

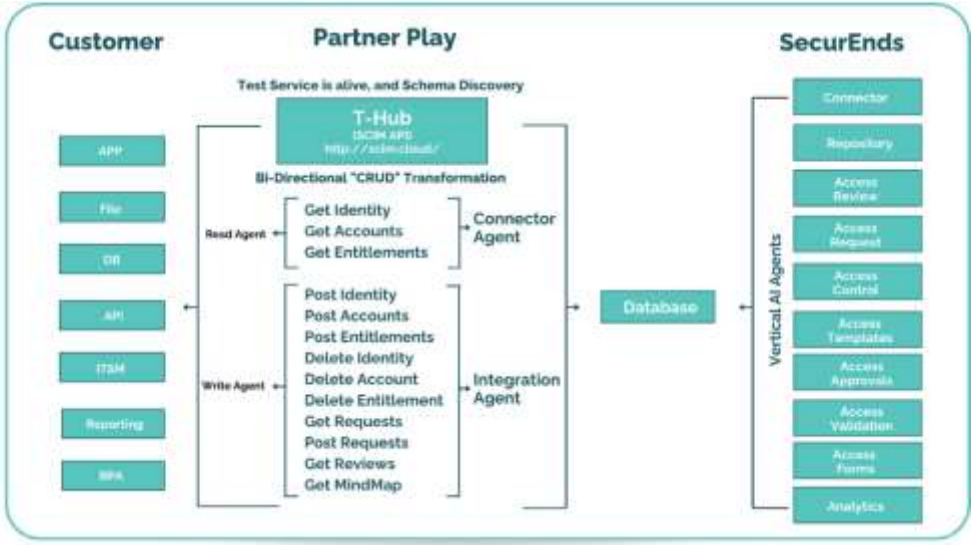
Access Request Template

Templates simplify and standardize access provisioning by enforcing Role-Based Access Control (RBAC). Instead of handling access requests individually, organizations can leverage predefined templates to automate and streamline role-based access assignments. With Access Request Templates, users can request access based on their role rather than manually selecting individual permissions, ensuring consistent access provisioning across departments and reducing entitlement creep. This approach accelerates approval processes by aligning requests with predefined business roles and policies, minimizing security risks by eliminating ad-hoc or unnecessary access requests.

T-HUB : Connect Anything, Automate Everything

T-Hub is the flexible, language-independent integration hub from SecurEnds that empowers organizations to connect identity governance with any system—on-prem, SaaS, or custom-built. Built on SCIM and REST API standards, T-Hub acts as a middleware API gateway, enabling bi-directional data flow between SecurEnds and your application ecosystem.

Whether you're provisioning access to Active Directory, deprovisioning SaaS entitlements, pulling tickets from your ITSM, or syncing entitlement data from a legacy system—**T-Hub gets it done, without the need for expensive customization or consultants**



Features

Automate Provisioning and Deprovisioning: Push and pull user access changes in real-time to and from AD, Azure, Okta, or any custom system.

Connect to Any App, Any Way: Use Python, Java, or JavaScript to build lightweight workflows for apps with no native connector. Exchange data in JSON or XML.

Streamline Emergency Access with Control: Use API calls to enforce temporary, just-in-time access and automatically remove entitlements when no longer needed.

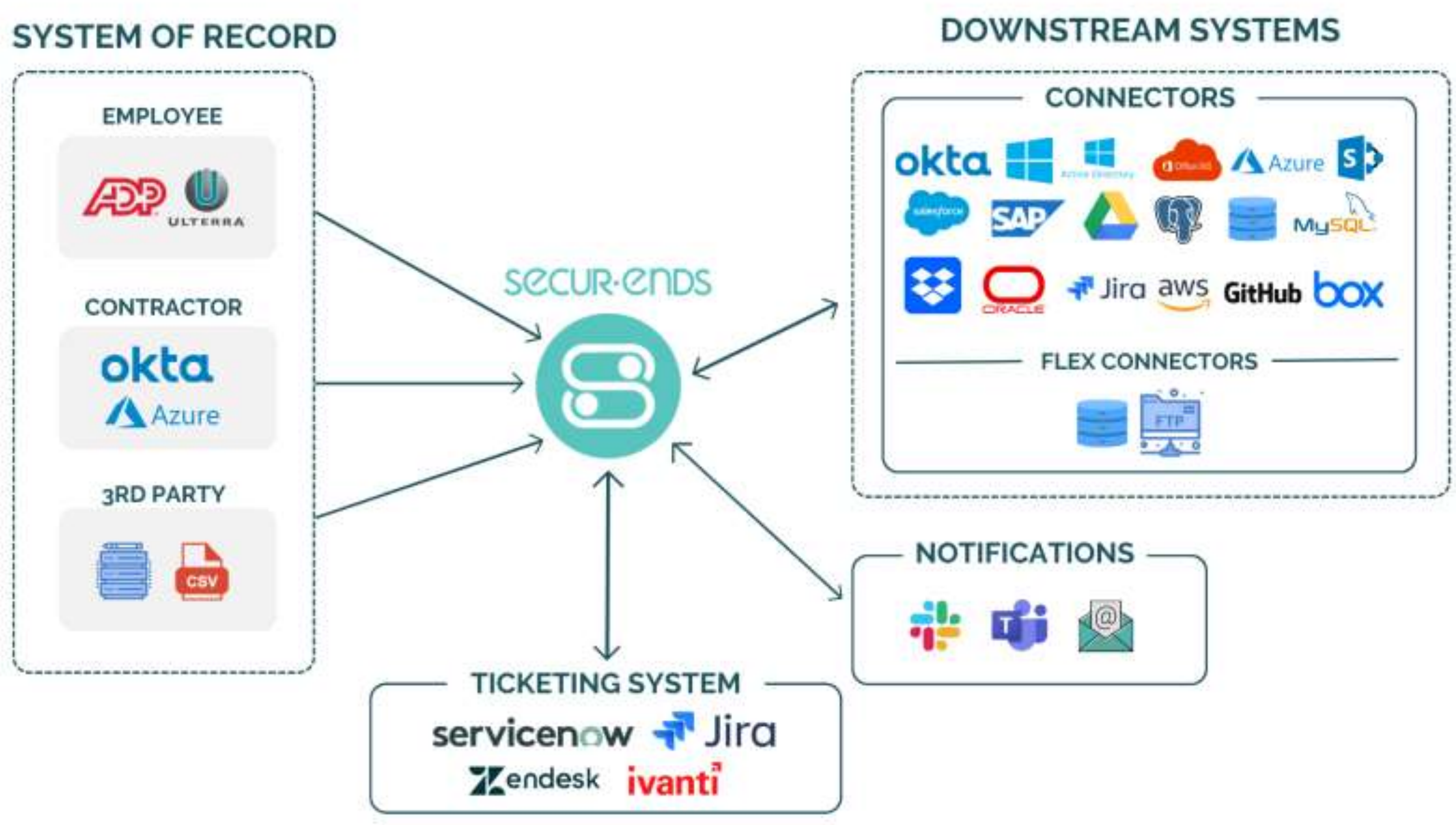
Leverage Approval Workflows : T-Hub operates outside of SecurEnds' governance engine, so you maintain business logic while enabling direct fulfillment.

Maintain Full Auditability: Capture who requested, who approved, and how access was fulfilled—everything tracked via request ID and available for export.

Support Any Identity Ecosystem: Whether it's a modern SaaS tool, a legacy database, a homegrown ERP, or an RPA bot—T-Hub bridges the gap.

Platform Overview

SecurEnds offers an industry leading SaaS product that automates laborious user access reviews, and streamlines the identification of orphan, overprovisioned and dormant employee, contractor and service accounts.



For illustrative purposes only as implementation varies from customer to customer

Value Drivers

Ease of use

Clean UI

No IAM expertise needed to run campaigns

Automate

Eliminate hours of previously manual reviews

Time to value

Cloud born

Deploy within weeks to manage risk quickly

Configurable

Flexible

Manage identities across apps using flex connectors

Versatile

Integrate directly into existing SSO application

Cost effective

Low implementation

Avoid costly multi-year implementation projects

SecurEnds GRC Modules

Cyber Security Risk Assessment/ Risk Management

This module is designed to identify, analyze, and mitigate potential risks to information systems, data assets, and technology infrastructure. This module provides a comprehensive and systematic approach to managing cybersecurity risks, ensuring the confidentiality, integrity, and availability of sensitive information.

Third Party Assessment

The SecurEnds Third-Party Risk Management module provides businesses with a comprehensive solution to assess, monitor, and mitigate risks posed by their vendors, suppliers, and partners.

Cloud Compliance

This module enables organizations to assess, evaluate, and ensure compliance with industry standards and regulations across cloud environments such as AWS (Amazon Web Services), Office (Microsoft Office 365), and GCP (Google Cloud Platform).

Privacy Management

This module offers organizations a comprehensive solution to effectively manage and uphold privacy regulations and standards such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other global privacy laws

Policy Management

This module provides organizations with a comprehensive solution to establish and maintain a centralized repository of policies, ensuring consistency and alignment with regulatory requirements and industry best practices.

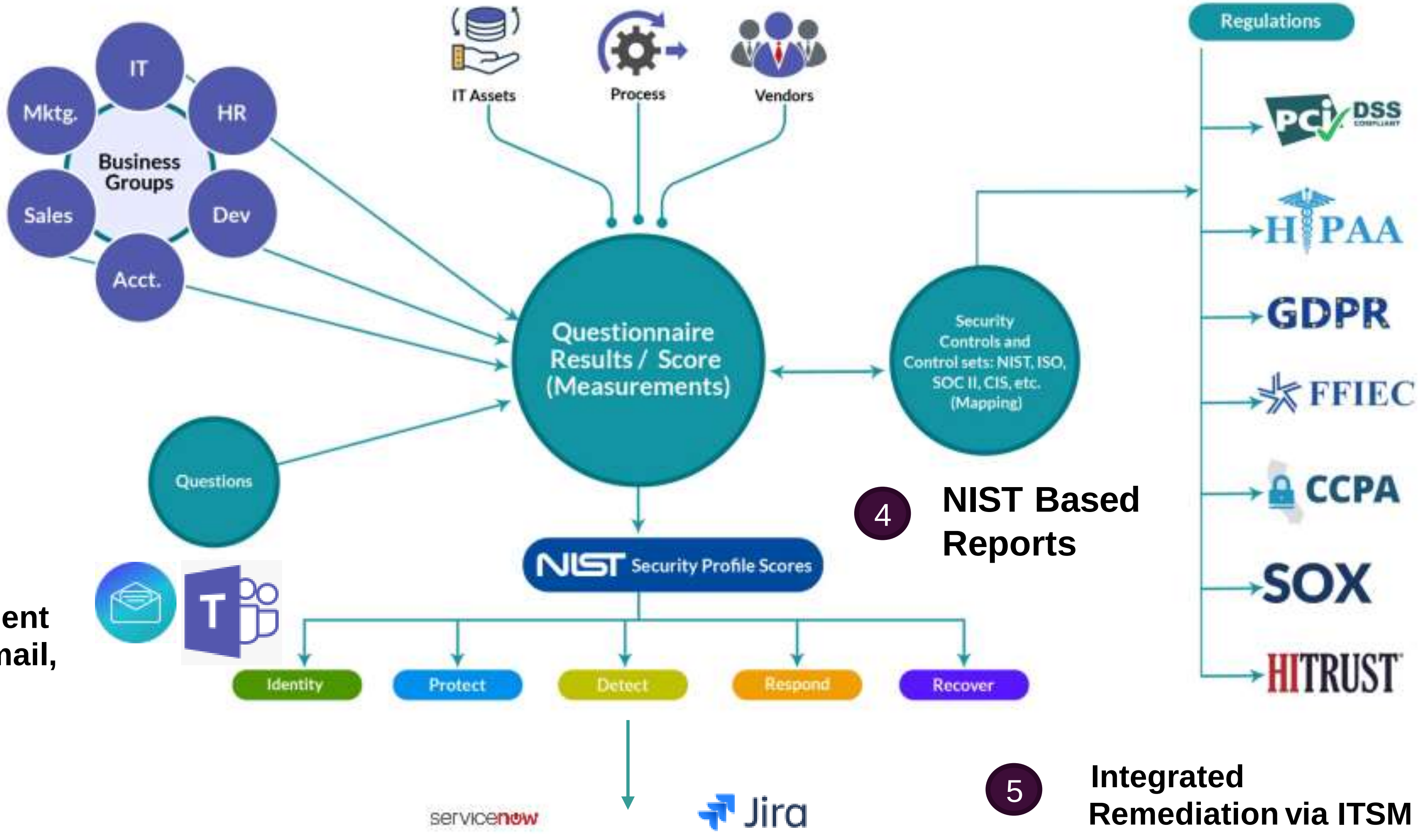
Business Continuity Planning

This module enables businesses to develop, implement, and maintain robust business continuity plans to prepare for and respond to potential disruptions and disasters, ensuring the continuity of critical business operations.

SecurEnds GRC Workflow

1 Create Assets Inventory

2 Select Assessment Framework & Assign Questions



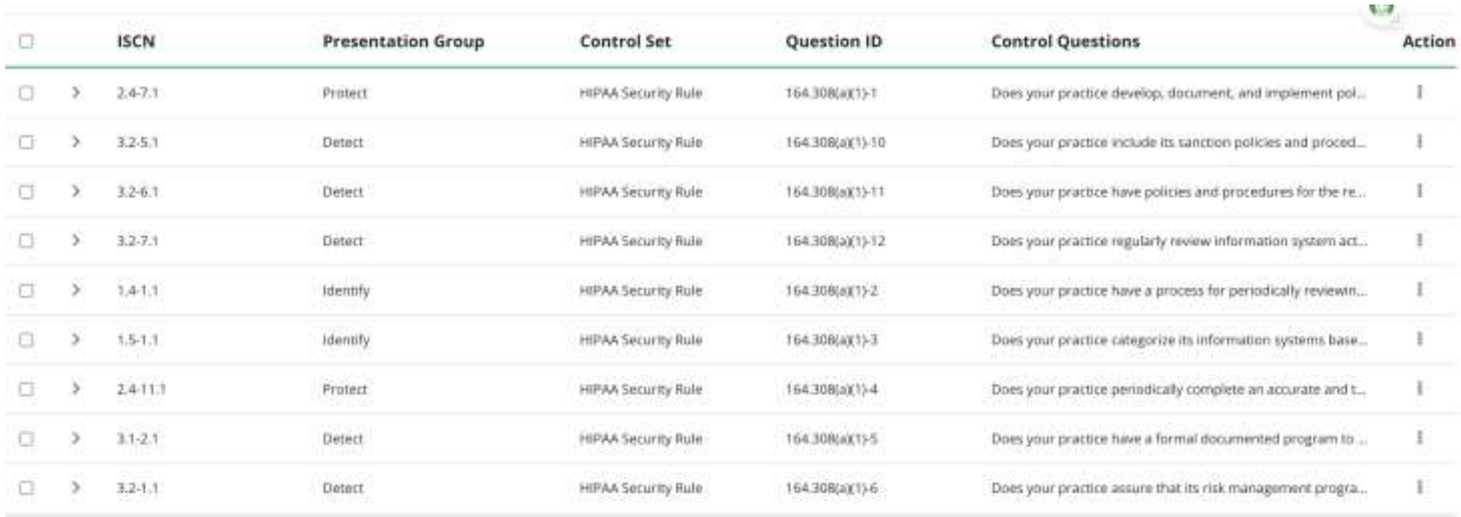
3 Run Assessment Campaign (Email, Teams)

4 NIST Based Reports

5 Integrated Remediation via ITSM

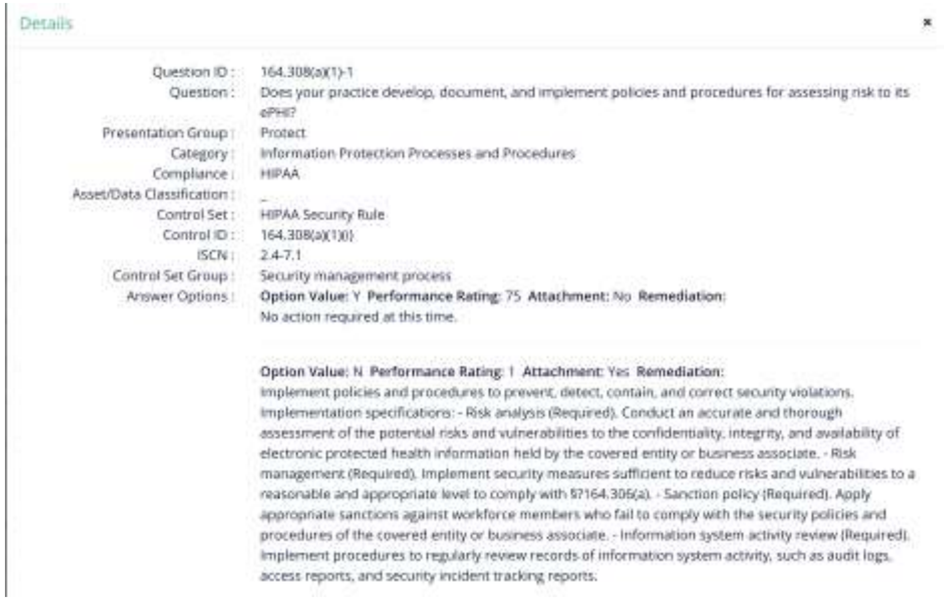
SecurEnds GRC Features

Zero Set-Up : Hit the ground running on Day 1 with prebuild security control templates that lead to a security assessment with questionnaires, workflows and inventory.



□		ISCN	Presentation Group	Control Set	Question ID	Control Questions	Action
□	›	2.4-7.1	Protect	HIPAA Security Rule	164.308(a)(1)-1	Does your practice develop, document, and implement pol...	⋮
□	›	3.2-5.1	Detect	HIPAA Security Rule	164.308(a)(1)-10	Does your practice include its sanction policies and proced...	⋮
□	›	3.2-6.1	Detect	HIPAA Security Rule	164.308(a)(1)-11	Does your practice have policies and procedures for the re...	⋮
□	›	3.2-7.1	Detect	HIPAA Security Rule	164.308(a)(1)-12	Does your practice regularly review information system act...	⋮
□	›	1.4-1.1	Identify	HIPAA Security Rule	164.308(a)(1)-2	Does your practice have a process for periodically reviewin...	⋮
□	›	1.5-1.1	Identify	HIPAA Security Rule	164.308(a)(1)-3	Does your practice categorize its information systems base...	⋮
□	›	2.4-11.1	Protect	HIPAA Security Rule	164.308(a)(1)-4	Does your practice periodically complete an accurate and t...	⋮
□	›	3.1-2.1	Detect	HIPAA Security Rule	164.308(a)(1)-5	Does your practice have a formal documented program to ...	⋮
□	›	3.2-1.1	Detect	HIPAA Security Rule	164.308(a)(1)-6	Does your practice assure that its risk management progra...	⋮

Customizable Controls Library: Fully customizable, out of the box questionnaires tied to standard controls such as NIST CSF, 800-53 & 800-171, ISO 27K, HIPAA, FFIEC, and other industry requirements. A single template leading to compliance can be used across all teams and departments, minimizing the number of questionnaires.

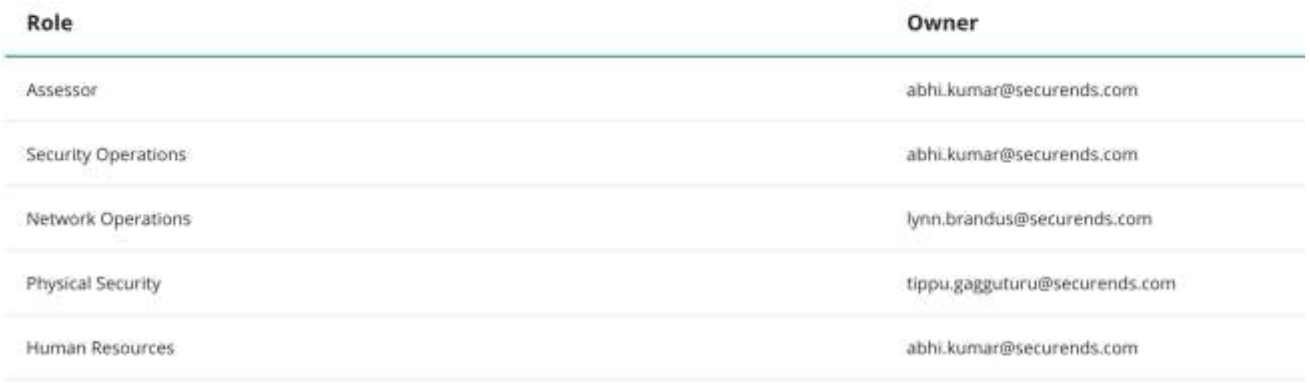


Question ID : 164.308(a)(1)-1
Question : Does your practice develop, document, and implement policies and procedures for assessing risk to its ePHI?
Presentation Group : Protect
Category : Information Protection Processes and Procedures
Compliance : HIPAA
Asset/Data Classification : _
Control Set : HIPAA Security Rule
Control ID : 164.308(a)(1)(i)
ISCN : 2.4-7.1
Control Set Group : Security management process
Answer Options : **Option Value:** Y **Performance Rating:** 75 **Attachment:** No **Remediation:**
No action required at this time.

Option Value: N **Performance Rating:** 1 **Attachment:** Yes **Remediation:**
Implement policies and procedures to prevent, detect, contain, and correct security violations. Implementation specifications: - Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. - Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §?164.306(a). - Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. - Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

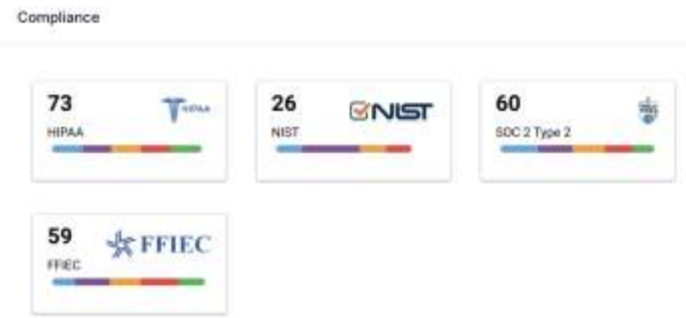
SecurEnds GRC Features

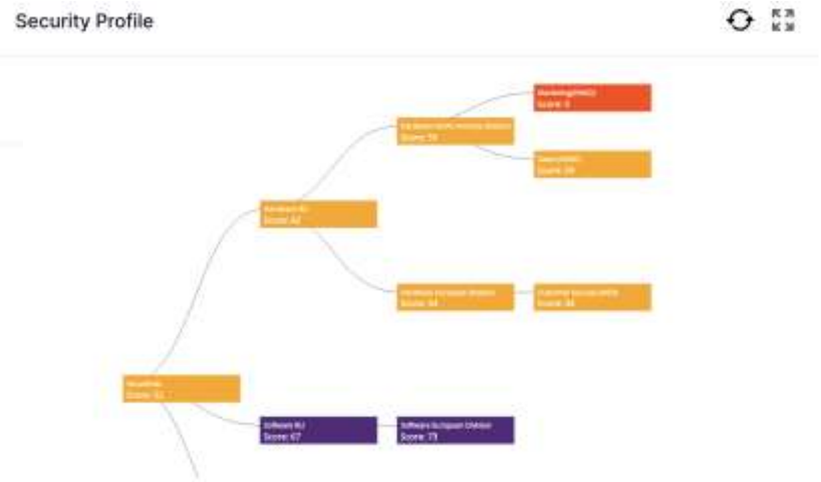
Role Based Assessment : Once roles are established, specific individuals can be assigned to handle particular sets of questions, ensuring that they have access only to the questions relevant to their designated responsibilities.



Role	Owner
Assessor	abhi.kumar@securends.com
Security Operations	abhi.kumar@securends.com
Network Operations	lynn.brandus@securends.com
Physical Security	tippu.gagguturu@securends.com
Human Resources	abhi.kumar@securends.com

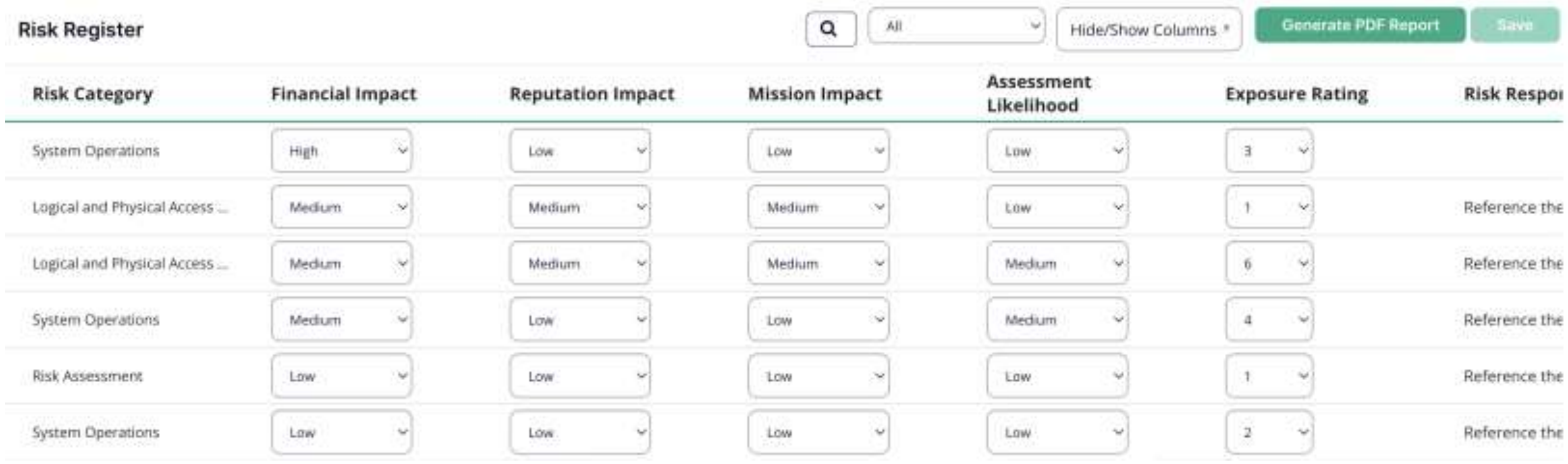
Risk Reports & Dashboard: Drill down reports on specific risk scores and controls, department risks, and remediation owners. Single-click "proof of compliance" and "executive dashboard" reports for auditors and management.





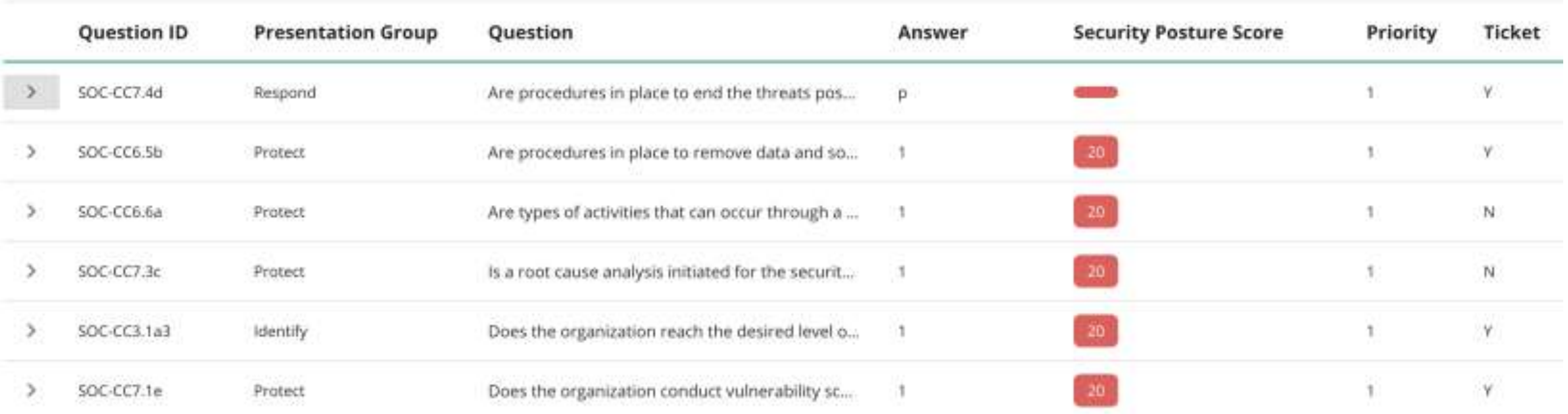
SecurEnds GRC Features

Risk Register: Use a scalable risk scoring system that quantifies the impact and likelihood of identified risks. This enables organizations to prioritize and focus on mitigating the most critical risks, optimizing resource allocation



Risk Category	Financial Impact	Reputation Impact	Mission Impact	Assessment Likelihood	Exposure Rating	Risk Respo
System Operations	High	Low	Low	Low	3	
Logical and Physical Access ...	Medium	Medium	Medium	Low	1	Reference the
Logical and Physical Access ...	Medium	Medium	Medium	Medium	6	Reference the
System Operations	Medium	Low	Low	Medium	4	Reference the
Risk Assessment	Low	Low	Low	Low	1	Reference the
System Operations	Low	Low	Low	Low	2	Reference the

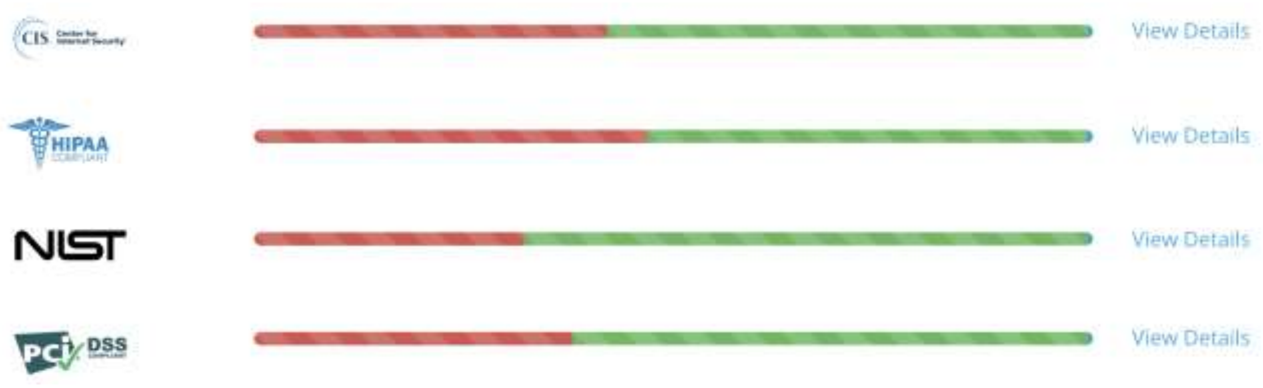
Remediations: Out of the box integrations with standard ITSM systems (Jira, ServiceNow, etc.) allows real-time assignment and monitoring of remediation tickets across internal and external risk owner

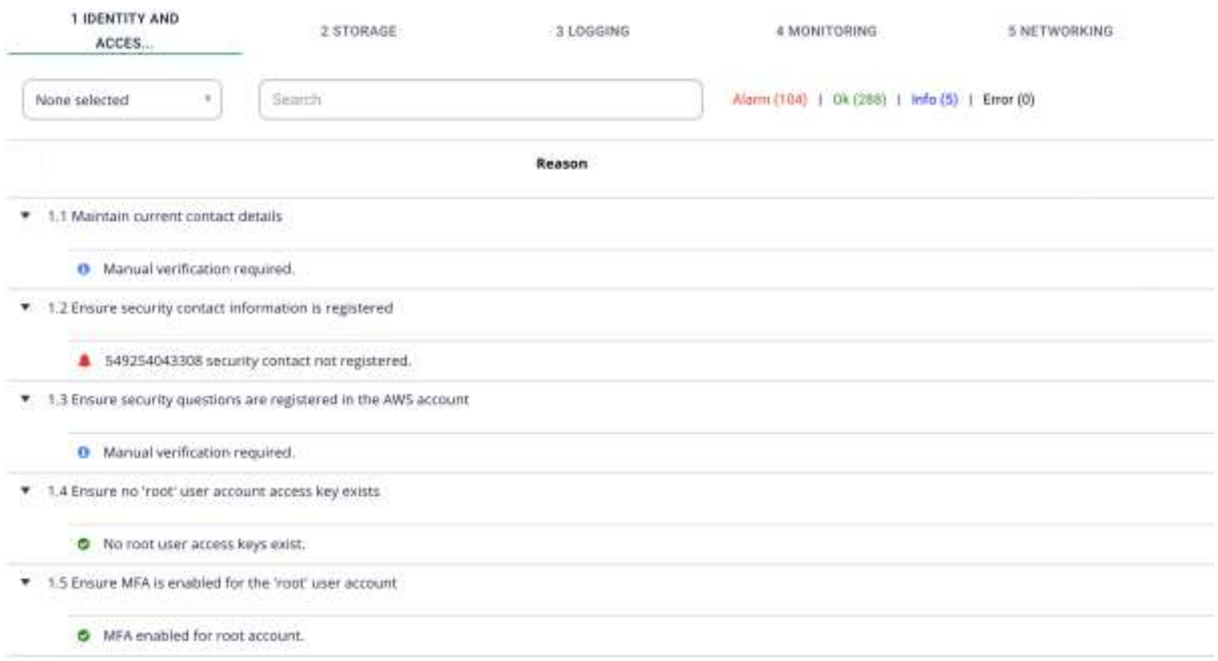


	Question ID	Presentation Group	Question	Answer	Security Posture Score	Priority	Ticket
>	SOC-CC7.4d	Respond	Are procedures in place to end the threats pos...	p	🟥	1	Y
>	SOC-CC6.5b	Protect	Are procedures in place to remove data and so...	1	20	1	Y
>	SOC-CC6.6a	Protect	Are types of activities that can occur through a ...	1	20	1	N
>	SOC-CC7.3c	Protect	Is a root cause analysis initiated for the securit...	1	20	1	N
>	SOC-CC3.1a3	Identify	Does the organization reach the desired level o...	1	20	1	Y
>	SOC-CC7.1e	Protect	Does the organization conduct vulnerability sc...	1	20	1	Y

SecurEnds GRC Features

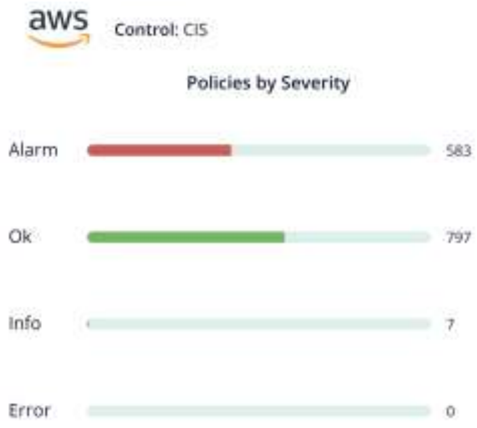
Cloud IaaS Audit: Audit the configuration settings of cloud IaaS (AWS, GCP, Azure) resources to ensure alignment with standard regulations (CIS, HIPAA, NIST, PCI etc).





Alarm (104) | Ok (288) | Info (5) | Error (0)

Reason
▾ 1.1 Maintain current contact details
Manual verification required.
▾ 1.2 Ensure security contact information is registered
549254043308 security contact not registered.
▾ 1.3 Ensure security questions are registered in the AWS account
Manual verification required.
▾ 1.4 Ensure no 'root' user account access key exists
No root user access keys exist.
▾ 1.5 Ensure MFA is enabled for the 'root' user account
MFA enabled for root account.



Thank You

secur·ends