SECUR ENDS

DATASHEET

CREDENTIAL ENTITLEMENT MANAGEMENT

Automate User Access Reviews

Achieve Compliance | Remove Orphaned Accounts| Enforce Principle Of Least Privileges

SecurEnds Credential Entitlement Management (CEM) enables organizations to accelerate their compliance posture so they can meet immediate needs and strategic objectives including:

- **Eliminating time-consuming manual processes**
- **Assigning responsibility to unmanaged assets**
- **Revoking excess access**
- **Proving business impact**

User Access Reviews are a common requirement across security and privacy compliance mandates. Usually, the mandate requires organizations to "periodically" review all user entitlements and attest to maintaining the principle of least privilege. For example, many companies struggle trying to comply with the Sarbanes-Oxley Act (SOX) compliance requirements.

Many organizations, even those with an Identity tool deployment, manage access certifications manually. They export their entitlement data to a spreadsheet, create pivot tables, send out emails to reviewers, and then track down reviewers who never responded.

40 %	72 %	47 %	82 %
Of organizations say the internal audit team spends too much time on SOX compliance duties	Of organizations use little or no data analytics in first line SOX control execution	Of organizations use their cloud service providers' identity and access management tools	Of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse, or simply an error

Meet Short- and Long-Term Compliance Requirements with Easy API-Based Integrations

With SecurEnds, companies can complete an initial deployment in as little as 4-6 weeks to start running certification campaigns and prepare audit documentation.

Our solution ingests all entitlements across an organization's environment, providing baseline visibility in days instead of months. Companies can use their current system or systems of record to start auditing entitlements so they can meet compliance deadlines. After gaining initial visibility, they can create workflows that help them meet long-term objectives.

SecurEnds ensures that organizations gain visibility into and control over:

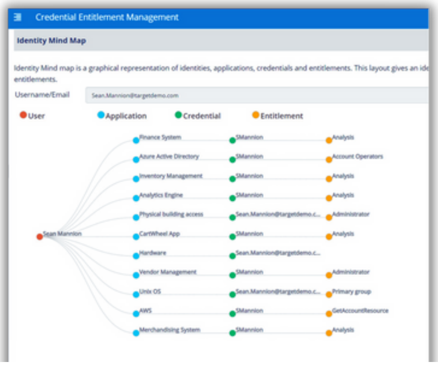
- Unassigned assets, like service accounts
- Multiple systems of record
- Excess access across complex, integrated environments

Gain At-a-Glance Visibility into Entitlements Across Complex Environments

Digital transformation creates complex, interconnected environments across on-premises, multi-cloud, and hybrid deployments. SecurEnds provides visibility into all entitlements so that organizations can reduce risk, document review, and enhance governance.

With SecurEnds, organizations can:

- Assign reviewers across IT or line of business
- Use identity-centric mind maps to see access and filter by user, application, credential, or entitlement
- Eliminate “rubber stamping”
- Transfer responsibility to appropriate reviewer



Credential Entitlement Management

Identity Mind Map

Identity Mind map is a graphical representation of identities, applications, credentials and entitlements. This layout gives an ide
entitlements.

Username/Email: Sean.Mannion@targetdemo.com

Demonstrate Business and Compliance Value by Measuring Campaign Success and Completion

For most companies, compliance is a time-consuming task that reduces time spent on activities that generate revenue. SecurEnds gives organizations a way to track campaigns and measure how compliance impacts security and business objectives.

- Track certification campaign completion status to reduce the time it takes to follow up with reviewers·
- Quickly provide easy-to-read documentation for internal and external auditors.
- Maintain remediation history to demonstrate the value compliance brings to security and business initiatives.
- Review historical effectiveness with metrics showing revoked entitlements.
- Quickly identify changes from previous campaigns with delta reports.
- Easily launch targeted certification campaigns with identity-based filters.

BENEFITS

01 Initial implementation in 4-6 weeks without requiring specialized skills to start running basic certifications for visibility into orphaned accounts, over privileged accounts, and obsolete accounts

02 Full visibility into all entitlements across on-premises, cloud, and hybrid deployments for accelerated review and compliance

03 Governance over traditionally unmanaged assets, like service accounts, by assigning responsibility and incorporating them into certifications

04 Enhanced security and compliance with frequent certification campaigns across mission-critical roles, including privileged user and service accounts

FEATURES

Single identity repository using fuzzy logic to match identities from multiple systems of record with credentials and entitlements across the organization

Identity-centric mind map that illustrates "who has access to what" with ability to filter by user, application, or entitlement

Out-of-box integrations with standard enterprise applications, SaaS applications and ability to pull data from legacy applications

Support multiple review types including direct manager, entitlement custodian, application manager, or ad-hoc reviewer

Centralized audit trail by logging approval/revoke decisions and reviewer notes with in-build ITSM-based remediation functionality

Delegate and/or reassign access reviews to additional reviewers if second level of attestation is required

About SecurEnds

SecurEnds' solution provides a single unified view across all applications and platforms, including cloud and on-premises. SecurEnds Credential Entitlement Management (CEM) automates access reviews, and our Governance, Risk, and Compliance (GRC) solution automates IT risk assessments. Our solutions reduce audit fatigue and security risk so organizations can document their answers to the critical questions of “who has access to what?” and “what is our security risk?”

Gain visibility today - visit **securends.com**!