KuppingerCole Report

EXECUTIVE VIEW

By Richard Hill
December 17, 2020

SecurEnds Credential Entitlement Management

Due to the potential impact of security risks arising from a lack of proper access governance controls, access governance has become a vital IAM technology for any organization. SecurEnds Credential Entitlement Management (CEM) simplifies user entitlement activities through automation and insightful analytics, giving organizations control of their user access governance.

By **Richard Hill**
rh@kuppingercole.com

Content

1 Introduction 3

2 Product Description 5

3 Strengths and Challenges 8

4 Related Research 10

Copyright 11

1 Introduction

Access Governance & Intelligence is an IAM focused risk management discipline that facilitates business involvement in the overall management of access rights across an organization's IT environment. Access governance provides necessary (mostly self-service) tools for businesses to manage workflows and access entitlements, run reports, access certification campaigns, and SOD checks. Access intelligence refers to the layer above access governance that offers business-related insights to support effective decision making and potentially enhance access governance. Data analytics and machine learning techniques enable pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection.

Access governance concerns the access mechanisms and their relationships across IT systems and is instrumental in monitoring and mitigating access-related risks. These risks most commonly include information theft and identity fraud through unauthorized changes or subversion of IT systems to facilitate illegal actions. During the last few years, many major security incidents originated from poorly managed identities, which established the need to address these issues across all industry verticals. Data thefts, loss of PII (Personal Identifiable Information), breach of customer's privacy, and industrial espionage are becoming common security risks in virtually every industry today.

Access Governance, an IAM focused risk management discipline, focuses on providing answers to a few key questions such as:

- Who has access to what and why?
- Who has approved that access?
- Are there any orphan accounts?
- Are there any dormant accounts?

These questions can be answered through a set of access governance functionalities, which includes warehousing access information from different systems, providing controls for attestation and recertification processes, auditing, reporting, and monitoring capabilities. In turn, these capabilities invoke active management of preventive controls to identify and mitigate the access risks. Additional aspects are data analytics for pattern recognition to drive process automation, effective role management, anomaly detection, and other access intelligence capabilities.

Another challenge today is that most organization IT data, applications, and services are spread across both on-premises and cloud environments. Inevitably there will still be business use cases that will ensure some IT data, applications, and services remain on-premises. In contrast, other use cases will drive the need to use cloud infrastructure and services, ensuring that this hybrid environment continues for the foreseeable future. Access governance solutions need to support both on-premises and cloud environments, which in many organizations are spread across multiple cloud vendors, in this hybrid reality. Many organizations also face the challenge of migrating from a data center to the cloud with a multi-cloud strategy. A multi-cloud strategy uses two or more cloud computing services such as AWS, Azure, and GCP.

SecurEnds addresses these challenges and risks through user access governance with its Credential Entitlement Management (CEM) solution. CEM leverages AI to automate user entitlement reviews across a wide range of applications and systems.

2 Product Description

SecurEnds is a disruptiptive technology vendor in the Access Management space. Their Credential Entitlement Management (CEM) solution offers a viable alternative to traditional Identity Governance. Born in the cloud, SecurEnds supports all major use cases for connected and disconnected applications. SecurEnds platform addresses organizations' Identity pain points by providing access governance such as, Access Certification, Cloud Identity Management and Governance, Access Control/Access Request, User Access Review/Access Certification, Seperation of Duty, and Identity Risk and Analytics (AI/ML) modules.

SecurEnds offers a cloud-based identity governance platform that sits between its customer's identity stores and the applications and services, whether on-premises or in the cloud.

Identity Integrations

The SecurEnds CEM allows for an identity system of record through connections to an organization’s authoritative sources of identities typically provided via a Human Resource database or directory. SecurEnds allows a variety of data consumption methods to obtain authoritative source identities, including out of the box connectors to a wide range of applications and services like Microsoft Active Directory, Azure Active Directory, Okta, API based HR systems, flat-files, and databases. Once all identity repositories are procured from authoratative sources, a consolidated view of all identities are made available within the SecurEnds unified identity database.

With CEM, customers can set up an automated post access review ticketing system action which will generate support tickets requiring remediation within an organization. Other configurations include access approval workflows for provisioning or de-provisioning to be executed automatically via an application connection, through a ticketing system such as ServiceNow, or through an email. SoD policy and access policy settings are also configurable through the Identities web UI.

Applications and Services Integration

Once a system of record is established within the SecurEnd CEM platform, data can be consumed from an enterprise applications (e.g., Salesforce or Active Directory), cloud services such as AWS, Azure, or even custom applications though available out-of-the-box connectors or through SecurEnds’ Flex-Connectors. Flex connectors are based on the OpenAPI specification, which can connect to databases, FTP folders, web APIs (e.g., REST), or even upload a JAR file or script to connect to an application and retrieve user entitlements as well as provisioning & de-provisioning. Application user information can also be imported into SecurEnds CEM via its connectors, or for more complex use cases, a file (e.g., Excel) can be imported when required.

SecurEnds uses AI/ML to match application credentials to the identities within the CEM unified identity database. An administrative view of all connected applications shows a list of each connected application and the number of matched, unmatched, excluded, deleted, or purged identities. For unmatched users, SecurEnds provides a fuzzy logic search based on user attributes such as first and last name, email, employee ID or UserID as examples for unmatched identities associated with applications. Once an unmatched credential is matched to an identity in the CEM database, SecurEnds remembers and automatically associates the identities and credentials for all future data syncs. Other actions that can be applied against listed applications include updating information, view application credentials, or entitlements.

Access Reviews

After the system of record is established and user applications are connected, managers can conduct user access reviews by roles or other attributes. Access review campaigns are created through campaign templates. These templates allow the grouping of applications and entitlements together for a given review campaign. Selected applications within the campaign can be drilled down further to specify the level of access to review. Delta campaigns can also be specified to allow an access review of only the changes since the most recent access review. Delegation of campaign reviews is possible if needed. For complex reviewer conditions, SecurEnds provides a rules engine where conditional rules can be specified. All other conditions of the access review campaign, such as review period, email notification, reminders, and escalations are also fully configurable. For active campaigns, a reviewer can approve, revoke, and add notes in a user-friendly web-based user interface.

Access review campaign reporting features include a graphical pie chart view of a given campaign's progress to highlight the percentage of pending, revoked, or approved entitlements. The graphs are interactive and administrators can drill down to view details of each component. Another important campaign report measures the effectiveness of post review remediation by reconciling access review election to updates applied to the source systems following a campaign. All-access review reports can be exported to PDF or CSV. Another interesting feature is the ability to audit historic campaigns by campaign name, application, and annual totals.

Separation of Duty (SoD) policies can be created, queried or SoD review campaigns can be conducted in a similar manner as the applications and entitlements access review campaigns.

Access Requests

User access requests can be made for both SSO and non-SSO applications. The user can select from an application catalog. Groups, roles, and applicable policies for a given application can also be specified. Once the access request is submitted, an email is sent to the respective application approvers. Pending requests can be view via a web-based dashboard showing pie chart statistics such as pending approvals, approval types, or the number of pending approvals greater than a month as examples. Within the same administrative interface, each request is itemized with the ability to approve or reject access requests.

Both groups and roles can be created through the Access Control section of the administrative UI. Groups can be created with one or more conditions, and roles can be associated with one or more applications. Both roles and groups can then be selected by the user when making an access request. Events can also be specified for a role or group, such as provisioning onboarding or offboarding.

Reporting, Analytics and Audit

The SecurEnds Identity Analytics module has many features, including mindmaps of identities and entitlements, as well as other AI/ML analytics. The identity mindmap graphically represents identities, applications, credentials, and entitlements with an identity-centric view across all entitlements and applications. As an example, for a given identity, all applications or services are listed. Selecting any of the user's applications will further expand to show all user groups, roles, or entitlements for that application. All graphical data can be exported for additional analysis or reporting.

The SecurEnds dashboards of its Identity Risk & Analytics solution provide interesting real-time graphics of user data. SecurEnds matches identities with user credentials across the enterprise using pattern matching fuzzy logic and behavior analytics from various sources. For example, it shows the identity risks, anomalies, inliers, and outliers.

Administration and DevOps Support

The SecurEnds Identity Management Platform is container-based for on-prem, cloud, and SaaS offerings. The SecurEnds Identity Management Platform is cloud-based but can extend to on-premises by using an agent that connects on-prem applications to the SecurEnds cloud service. In cases where the SecurEnds cloud service cannot be used, SecurEnds provides a Docker container of its software that can be deployed on-premises and connect to the on-prem applications. All connectors are currently RESTful API based, and third-party SCIM connectors are available as well.

The administration section of the SecurEnds platform allows for the configuration of roles, risk score, ticketing system for access reviews, emails, reviewer notes, and user interface configuration. The SecurEnds risk engine can be configured to use attributes such as employee, server, environment, or application data classification types as some examples.

3 Strengths and Challenges

SecurEnds is an emerging product built using a modular architecture, support for both on-premise and cloud deployment, intuitive UI for end users. All primary Identity Governance uses cases are covered. SecurEnds Identity Management Platform is used by both mid-market and enterprise organizations. SecurEnds Credential Entitlement Management (CEM) is capable of managing access requests, access notifications, access reviews, and certifications.

SecurEnds provides a wide range of connectors to the most common and popular identity repositories and user applications and services. It supports multi-vendor cloud identity solutions out of the box. SecurEnds Flex-Connectors provide a strategic alternative for more complex connection use cases, such as connections to legacy systems. Also, SecurEnds provides its own system of record MySQL database integrated within the product. However, SecurEnds does not offer a SCIM interface for external applications.

A good set of AI/ML and analytic module capabilities are given when bundled with SecurEnds CEM. The visual identity and entitlement mindmaps provide a useful way to view and drill down to access specific information. Although integration support for other third-party risk engine solutions is not available, the risk engine offered with the SecurEnds CEM solution is quite versatile and capable of identifying a variety of risk based on a range of attributes.

SecurEnds CEM gives good self-service access request and access review functionality. Access review campaigns are easily configurable . An interesting delta campaign feature is also available, which can potentially save management time by not having to review all user access for each review period, but only the changes since the last review. The ability to conduct a separate SoD review campaign is also given. Although delegation of review campaigns can be configured during campaign creation, the option to forward or delegate an approval decision for a given user within the campaign is not given. Good attention to access review campaign reporting features is offered as well.

Overall, SecurEnds Credential Entitlement Management provides the access governance capabilities for the mid-market and larger enterprise organizations looking for a fully integrated Identity suite. SecurEnds continues to be a vendor to watch for its innovation and technology in the access governance market.

Strengths

- Wide range of out-of-the-box connectors to applications and services
- SecurEnds Flex connector supports more complex connection use cases
- Good access review capabilities
- Offers AI/ML and analytics feature set for access governance
- Container-based for on-prem, cloud, and SaaS deployments
- Intuitive workflows and modern UI provides for ease of adoption
- Modular and scalable appliance-based architecture

Challenges

- Partner ecosystem in early stages
- Consolidated identity database is integrated, disallowing integrations with other databases
- Integration support for other third-party risk engine solutions is not available
- Reliance on third-party SCIM connectors

4 Related Research

Advisory Note: KRIs and KPI for Access Governance - 72559
Architecture Blueprint: Access Governance and Privilege Management - 79045
Leadership Compass: Access Governance - 80098
Whitepaper: A Lean Approach on Identity & Access Governance - 80048

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.