SOLUTION BRIEF

Securonix Identity and Access Analytics

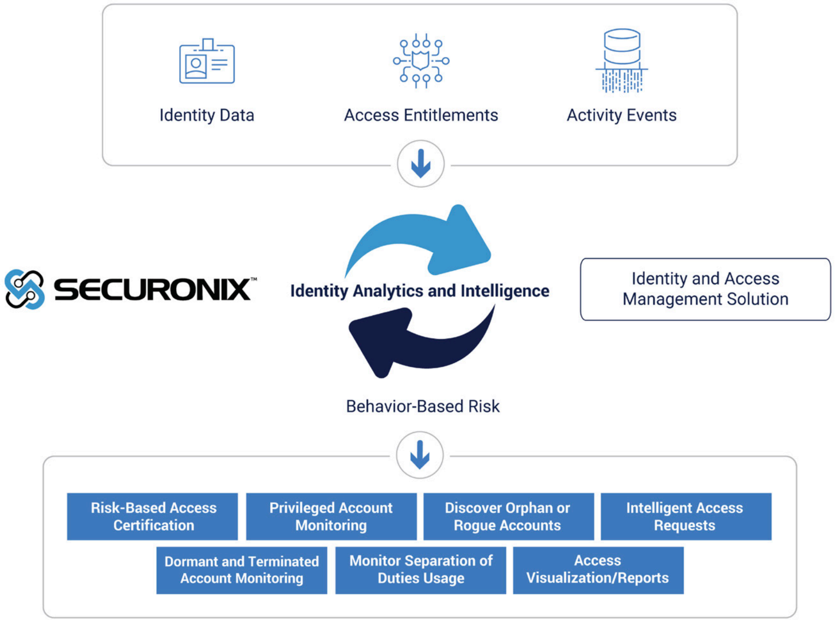
Traditionally, identities are managed using dedicated identity and access management (IAM) and identity governance and administration (IGA) solutions. This made sense when enterprise applications were in on-premises data centers. However, enterprise application data today rests in on-premises and cloud datastores. With multiple access privileges to manage for each user across a multitude of applications, organizations struggle to keep their access-related risk in check.

To address this challenge, Securonix applies advanced behavior analytics to identity usage and access patterns in data collected from IAM solutions such as Saviynt, Okta, Ping Identity, and SailPoint. This enables the creation of risk profiles for user behaviors, which can be used by the IAM solution to make dynamic, informed access decisions. The integrated solution delivers advanced identity analytics and intelligence capabilities, enabling several use cases that are otherwise difficult for IT security teams to manage.

Better Access Control and Efficiency

Securonix integrates with every major IAM and IGA solution to deliver a continuous stream of identity analytics and intelligence allowing for:

- Improved access management compliance through user- and resource-centric views of access risk.
- Automated access cleanup and risk-based certification.
- Streamlined, risk-based access request processes.

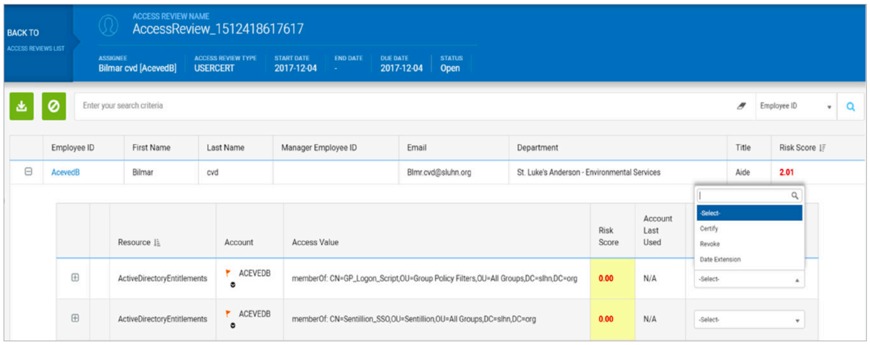

Identity Data
Access Entitlements
Activity Events
SECURONIX
Identity Analytics and Intelligence
Identity and Access Management Solution
Behavior-Based Risk
Risk-Based Access Certification
Privileged Account Monitoring
Discover Orphan or Rogue Accounts
Intelligent Access Requests
Dormant and Terminated Account Monitoring
Monitor Separation of Duties Usage
Access Visualization/Reports

Solution Benefits

- Streamlined, direct integration with multiple identity management partners.
- The Securonix platform performs user behavior analytics on identity usage and access patterns identified by IAM tools. This enables the creation of risk profiles for user behaviors, which can be used in context by the IAM tool to make dynamic, informed access decisions.
- Enrich data with additional context.

Risk-Based Access Certifications

Access certifications are a necessary evil. They are required to ensure that user privileges are not over-assigned, but they can be work-intensive. Using analytics Securonix prioritizes high-risk user entitlements for certification, reducing workloads by over 90% and eliminating rubber-stamped access assignments.



BACK TO ACCESS REVIEWS LIST

ACCESS REVIEW NAME
AccessReview_1512418617617

ASSIGNEE	ACCESS REVIEW TYPE	START DATE	END DATE	DUE DATE	STATUS
Bilmar cvd [AcevedB]	USERCERT	2017-12-04	-	2017-12-04	Open

Enter your search criteria — Employee ID

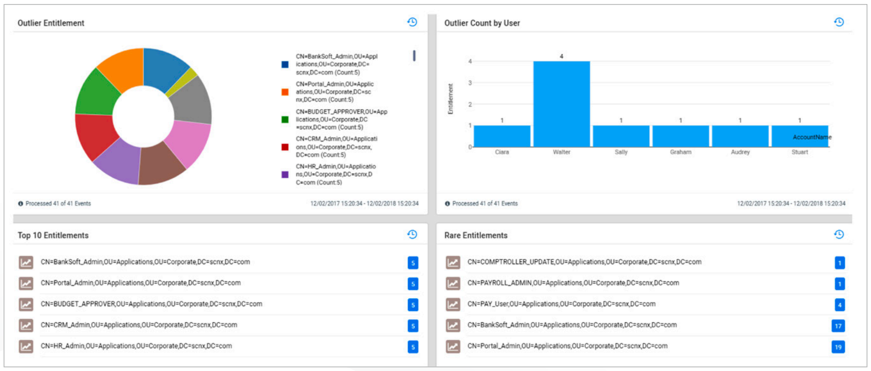
Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Risk Score
AcevedB	Bilmar	cvd		Blmr.cvd@sluhn.org	St. Luke's Anderson - Environmental Services	Aide	2.01

Resource	Account	Access Value	Risk Score	Account Last Used	
ActiveDirectoryEntitlements	ACEVEDB	memberOf: CN=GP_Logon_Script,OU=Group Policy Filters,OU=All Groups,DC=slhn,DC=org	0.00	N/A	-Select-
ActiveDirectoryEntitlements	ACEVEDB	memberOf: CN=Sentillion_SSO,OU=Sentillion,OU=All Groups,DC=slhn,DC=org	0.00	N/A	-Select-

Comprehensive Identity and Account Analytics

To enable a complete view into identity and user account based security issues, Securonix offers key capabilities, including:

- Risk-based access certification analysis.
- Fully customizable dashboards for raw and outlier entitlements.
- Thorough search and analytics on entitlement distribution within departments across the organization.
- Privileged account monitoring of administrative and service accounts for suspicious activities.
- Peer inlier reporting for identifying common peer group permissions.
- Dormant and terminated account analytics.



Outlier Entitlement
CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com (Count:5)
CN=Portal_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com (Count:5)
CN=BUDGET_APPROVER,OU=Applications,OU=Corporate,DC=scnx,DC=com (Count:5)
CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com (Count:5)
CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com (Count:5)
Processed 41 of 41 Events
12/02/2017 15:20:34 - 12/02/2018 15:20:34
Outlier Count by User
Entitlement
0
1
2
3
4
1
4
1
1
1
1
AccountName
Ciara
Walter
Sally
Graham
Audrey
Stuart
Processed 41 of 41 Events
12/02/2017 15:20:34 - 12/02/2018 15:20:34

Top 10 Entitlements

CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	5
CN=Portal_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	5
CN=BUDGET_APPROVER,OU=Applications,OU=Corporate,DC=scnx,DC=com	5
CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	5
CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	5

Rare Entitlements

CN=COMPTROLLER_UPDATE,OU=Applications,OU=Corporate,DC=scnx,DC=com	1
CN=PAYROLL_ADMIN,OU=Applications,OU=Corporate,DC=scnx,DC=com	1
CN=PAY_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	4
CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	17
CN=Portal_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	19

Key Use Cases

- Detect excessive user permissions.
- Enable risk-based access clean-up and certification.
- Monitor privileged and service account usage.
- Detect segregation of duty (SOD) anomalies.
- Discover rogue or orphan accounts.
- Monitor for the usage of dormant and terminated accounts.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000