securonix

SOLUTION BRIEF

Securonix for Access Analytics

Detect and Respond to Credential-based Security Threats

Solution Benefits

Streamlined Integration

Securonix Next-Gen SIEM integrates with many major IAM and IGA solutions to deliver a continuous stream of identity analytics and intelligence.

Easier Access Management

Our solution takes the guesswork out of access management by streamlining access requests based on a user's risk level.

Gain Identity Context

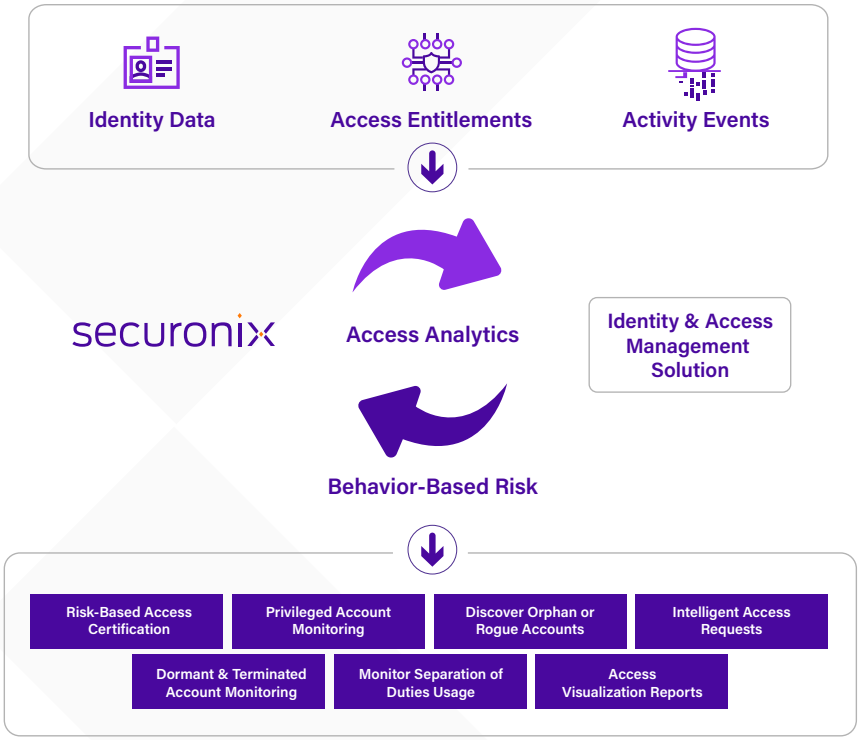
Take advantage of IAM and IGA context to identify user behavior that could indicate compromised or misused credentials.

Secure Your Modern Enterprise

According to The 2021 Verizon DBIR Report, 61% of breaches involve credentials, making the need for identity analytics a crucial part of staying ahead of cyber threats. Organizations are struggling to balance access and risk. They need to be able to make dynamic, informed access decisions by leveraging user risk intelligence with their IAM solutions.

Why Securonix?

To address this challenge, Securonix applies advanced behavior analytics to identify 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.



Top Use Cases

Monitor Privileged and Service Account Usage

Due to the high level of access privileged accounts are granted, they are often prime targets for cybercriminals. By monitoring privileged accounts using identity analytics and intelligence, unusual behaviors such as privilege escalations, data exfiltration, credential sharing, and account compromise can be detected and resolved before larger damage is done.

Detect Excessive Permissions

Giving a group of users excessive permissions – without considering their specific position gives hackers more entry points into your organization. Securonix minimizes risk by monitoring access trends and correlating the data with user profiles from your IAM solution. The resulting analytics help you determine what level of permission is needed for each user and helps eliminate the risk of granting excessive permissions that can be abused.

Discover Rogue or Orphaned Accounts

Rogue and orphaned accounts with high-level privileges often go unnoticed and are ripe for compromise. Using identity analytics and intelligence, you can correlate actions that previously weren't traceable back to specific accounts or entitlements. Our solution's analytics enable you to revoke access to these accounts, increasing your security posture while lowering licensing expenses.

Monitor Usage of Dormant and Terminated Accounts

Dormant and terminated accounts need to be purged on a regular basis but are easily overlooked. Securonix Access Analytics detects unusual activities and alerts you to revoke privileges for dormant and terminated accounts. By reducing the possibility of credential misuse, you can minimize the risk these accounts pose to your organization.

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo