Anetac's Streaming Identity Vulnerability and Security Platform

Modern identity security vulnerability challenges are dynamic, necessitating a continuous solution. **Anetac is a streaming identity vulnerability and security platform** that excels in accurate discovery, monitoring and response for a wide range of identities, such as service accounts, human, API keys, access keys and tokens. Using Anetac's dynamic solution, organizations can effectively and thoroughly elevate an organizations security posture by increasing the efficacy of existing IAM and CMDB tools.

"With Anetac, we discovered a service account where the creator retired before the account did"
- Global Insurance Provider

- Discover underlying problems with accounts
- Monitor ongoing behavioral changes
- Assess account and resource access chains and their impact across the entire organization
- Classify accounts based on behavior
- Create contextually accurate response plans
- Leverage time-series component for zero-day learning period

Anetac has been designed from the ground up for behavioral identity and vulnerability protection. With real-time streaming, the platform provides a full understanding of the identity landscape and maps risk across any environment. Anetac is designed to look at vulnerabilities from both sides: hygiene and threat prevention, as they are two sides of the same issue.

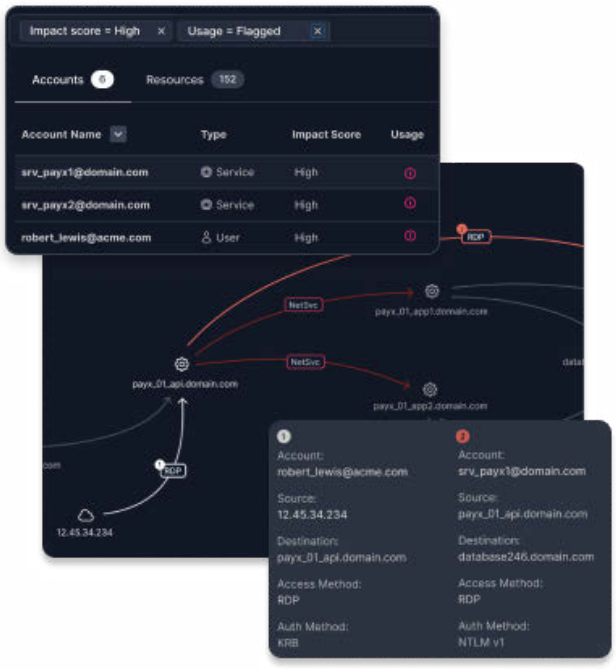
Anetac's Streaming Identity Vulnerability and Security Platform

anetac

Access Chains are formed during normal operations. For instance, a developer checking in code into GIT repository triggers a service account to create a binary, and push it to their AWS environment, where another service account is used to deploy the new binary and switches traffic.

This is all one access chain, each connection, each individual access method used, and each account used on each link of this chain tells a story. As each link of this chain has a different account, privileges, and access methods - it is dynamic across time.

Anetac discovers, analyses, and monitors these access chains for deviation, impact and change overtime to flag vulnerabilities before they become problems.



Anetac Project Examples

Authentication Protocols

Identifies authentication protocols and helps to eradicate the usage of weak access protocols within an organization

Privilege Escalations

Ongoing monitoring for untimely or suspicious privilege escalations and alerting for Identity related IoC(s) and IoA(s)

Account Detection

Discover lost, shadow and privileged dormant accounts that may not follow standard naming conventions

Credential Rotation

Secure organizations most critical assets by ensuring service accounts credentials are rotated

Real Customer Findings

102
Dormant Service Accounts over 10 years old

8.7 years
Average Password Age

19 years
Longest Service Account Dormancy age

24.7 years
Oldest Password Age

