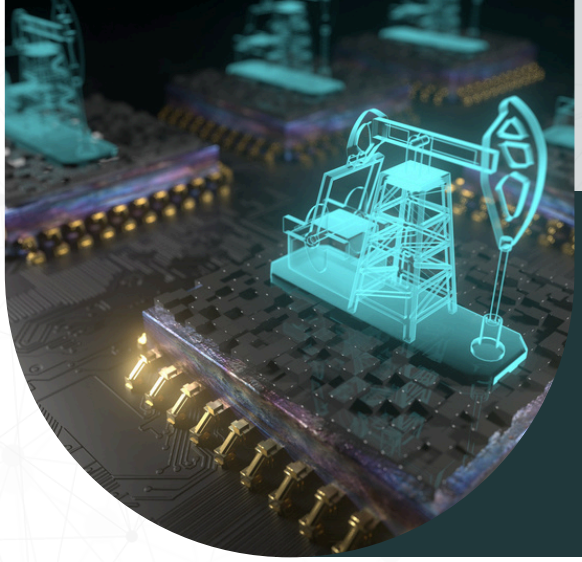


Case Study

DYNAMIC SERVICE ACCOUNT ASSESSMENT LINKS ASSETS FOR ZERO TRUST

Better security hygiene for 50k service accounts realized with streaming visibility, monitoring, and privilege chain analytics.

A worldwide mining organization was embarking on its journey towards implementing a robust zero-trust security framework and faced a significant challenge in gaining comprehensive insight into its service accounts. The lack of visibility into these accounts posed a considerable security risk, hindering the organization's progress toward achieving a trustworthy and secure digital environment. The organization recognized the importance of understanding and cleaning up its service accounts before implementing its zero-trust model.

Anetac's dynamic identity management platform delivered continuous, streaming visualization and mapping of the organization's entire service account landscape and their privilege chains. This enabled quick understanding of the dynamic and complex relationships between service accounts and essential resources, and illuminated potential attack paths and vulnerabilities.

COMPANY OVERVIEW

- Industry: Mining
- Size: ~3000 employees
- Location: Worldwide

"Anetac, literally, saved us 18 months of manual research on our service account landscape."

Executive, Worldwide Mining Organization

CHALLENGES BEFORE ANETAC

Lack of visibility

The organization had no comprehensive insight into its service accounts, leading to a vulnerability gap in its security posture.

Time-consuming manual process

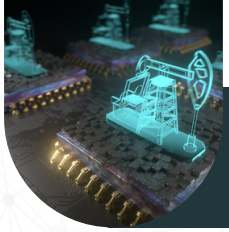
The manual process of sifting through logs for each account took 1-2 days just to create a short-lived map of an account. The effort required for account mapping was resource-intensive and time-consuming, hindering the organization's agility and responsiveness to emerging security threats.

Scale and Complexity

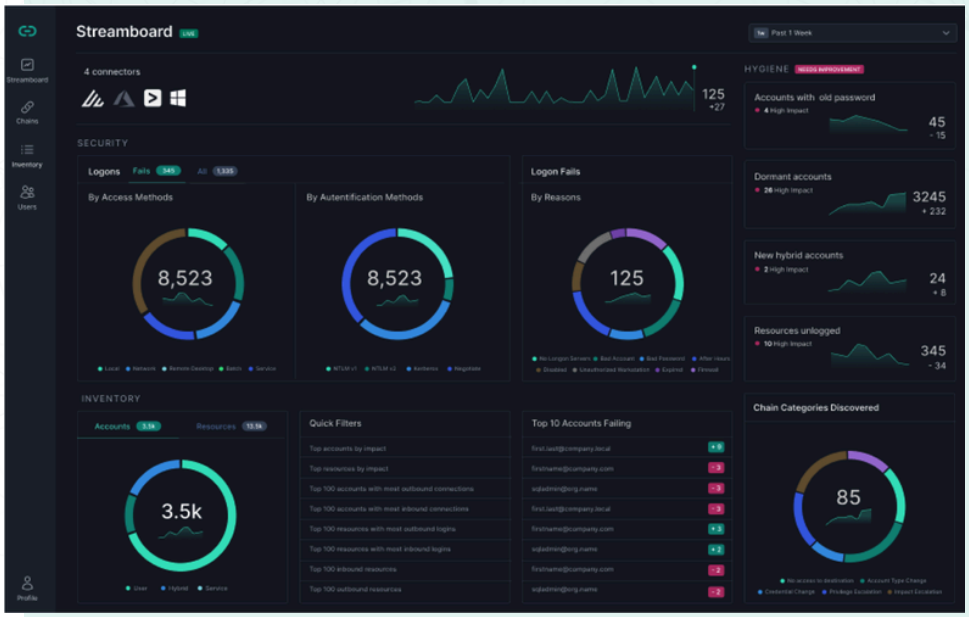
Managing a vast environment with over 50,000 accounts made it challenging to scale security efforts and maintain a comprehensive view of its service account landscape.

Incomplete Monitoring

The organization struggled to consistently monitor service accounts on an ongoing basis. The lack of continuous monitoring and accountability meant that potential security risks went unnoticed, leaving the organization vulnerable to threats.



anetac



IMPLEMENTATION

- Streamed collected inventory and event data into Anetac Cloud in less than an hour
- Time-to-value realized in 10 minutes with streaming privilege chain and account mapping visibility

WITH ANETAC

- Anetac helped create streaming visibility and mapping of the organization's entire service account landscape and its privilege chains.
- The organization was able to identify and monitor highly privileged, yet dormant, service accounts that had been categorized as active but remain unused (some with passwords over 365 days old).
- Anetac provided impact scores of each account, allowing the organization to focus first on accounts that posed a higher risk, such as those using NTLM or that had multiple login failures.
- The organization leveraged Anetac's rules, analytics, and artificial intelligence capabilities to continuously discover and monitor service account behavior across the enterprise.
- Anetac's behavioral analytics located and monitored mixed use (hybrid) accounts, continuously tracking the utilization of weak authentication protocols, failed login attempts, and old credentials.
- The Anetac platform streamlined reporting with 1-click reports that comprehensively documented and graphed the scope of any selected service account.

RESULTS

With Anetac, the customer mapped their service accounts with continuous, streaming visibility and are now quickly able to de-risk any changes to service accounts.