

Anetac's Dynamic Identity Vulnerability and Security Platform



Modern identity security challenges are constantly evolving, demanding a proactive and continuous solution. Anetac, **an award-winning leader in dynamic identity security**, delivers unparalleled accuracy in discovering, monitoring, and responding to identity vulnerabilities and understanding their **access chains**. Its cutting-edge platform safeguards a wide range of identities, from **non-human identities (NHIs)** like service accounts, API keys, access keys, and tokens to **human identities** such as third-party suppliers, contractors and partners. By seamlessly integrating with existing IAM and CMDB tools, Anetac enhances security posture, ensuring organizations stay ahead of emerging threats.

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

Comprehensive Dynamic Human and Non-Human Identity Security
Proactive Access Chain Monitoring

Evaluate Account and Resource Access Chains to Uncover Risks and their Organization-Wide Impact

Discover Orphaned or Dormant Accounts Across Human and Non-Human Identities

Effortlessly Enforce and Remediate Password Rotation Policies

Anetac was built along side security executives to tackle real-world identity security challenges. Designed for behavioral identity protection and vulnerability management, it leverages real-time streaming to map risks across your environments. Trusted by worldwide organizations across all industries, Anetac addresses vulnerabilities holistically; tackling both hygiene and threat prevention as two sides of the same challenge.



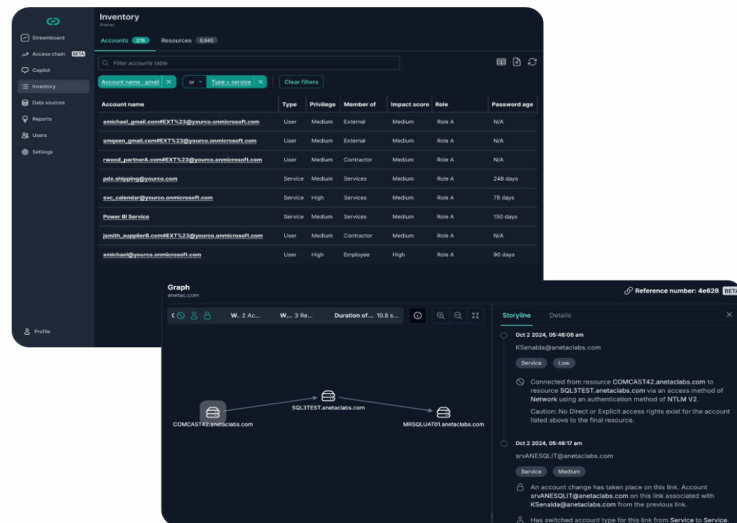
Anetac's Dynamic Identity Vulnerability and Security Platform



Access chains naturally form during routine operations. For example, when a developer checks code into a Git repository, a service account triggers the creation of a binary, which is then pushed to an AWS environment. Another service account deploys the binary and switches traffic.

This entire process forms a single access chain, with each connection, access method, and account contributing to its structure. Since each link in the chain involves different accounts, privileges, and access methods, the chain remains dynamic over time.

Anetac continuously discovers, analyzes, and monitors these access chains for deviations, impacts, and changes—proactively identifying vulnerabilities before they become threats.



Anetac in Action - Project Examples

Mitigate Service Account Misuse

Strengthen governance and discover privilege escalation, dormant accounts, and security vulnerabilities

Enhance Access Chain Visibility

Gain real-time visibility into direct and indirect access, and third-party supply chain risks

Secure Third-Party Supply Chain Accounts

Continuously monitor and manage account lifecycles to eliminate orphaned, unauthorized and out of policy access

Eliminate Weak Encryption and Insecure Protocols

Enforce strong encryption and secure protocols to protect administrative accounts from threat

Real Customer Findings

102

Dormant Service Accounts over 10 Years

19
Years

Longest Service Account Dormancy

8.7
Years

Average Password Age

24.7
Years

Oldest Password Age

