Continuously Discover, Monitor, and Respond to Service Account Risks

anetac

Anetac is a dynamic identity and security management platform that continuously discovers, monitors, and controls privileges for service accounts. It provides streaming visibility into privilege chains and protects access to essential resources. Service accounts are privileged, non-human accounts that are commonly used for automated tasks or for allowing applications to interact with other systems. Due to their often privilege access to sensitive data and software pervasiveness, service accounts are more vulnerable and constitute a critical attack surface that needs to be managed. Service accounts are hard to detect and map making them a prime vector for attackers.

Anetac helps to uncover blind spots with dynamic visualization of service account chains.

- Complete discovery of service accounts
- Monitor service account behaviors
- Understand access chains and paths between essential resources
- Streaming visualization of service account chains
- Easily identify service account relationships
- Get started and see value within one week

Discover Every Service Account Anetac continuously monitors your environment uncovering all service accounts—user, service and hybrid—while mapping privilege chains. Anetac uses behavioral analytics to discover service accounts, providing a complete view of the service account landscape, even if the organizational naming conventions are not followed.

Anetac leverages visibility of access chains and behavioral analytics to discover all service accounts and categorize them as user, service, or shared use accounts while continuously monitoring usage and access chain mapping.

Continuously Discover, Monitor, and Respond to Service Account Risks

anetac

Anatec Streamlines Service Account Identity and Security Management

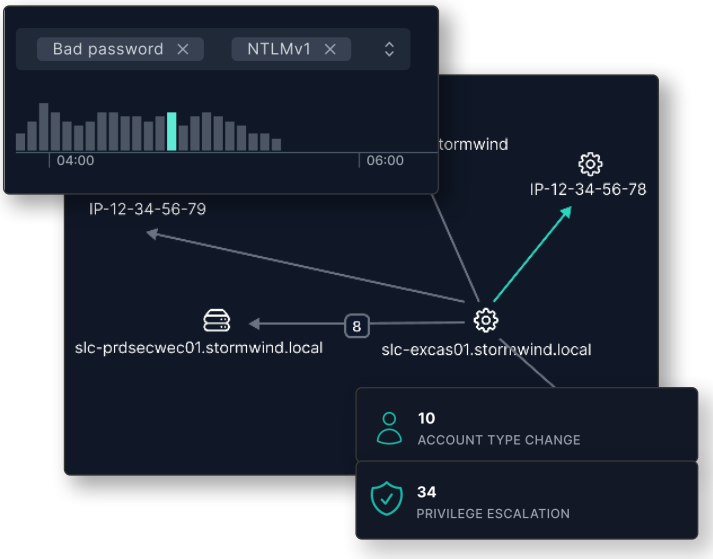
Continuous Service Account Chain Monitoring
Provides streaming monitoring of account behaviors.

Event Analysis
Anetac's streaming visualizations reveal the complex relationships between service accounts and essential resources, illuminating potential attack paths and vulnerabilities.

SaaS-based & Agentless
Quick and easy setup provides visibility to your service account landscape in minutes.

Flexible Deployment
Deploys to both on-premise and cloud environments without agents.

Graph & Privilege Chain Visualizations
Provides quick analysis of complex data patterns and relationships, improving decision-making and enhancing data analysis..



Contextual & Behavioral Insights
Integrates with your organization's existing environmental, contextual, and inventory data, such as Active Directory, for actionable insights.

Impact Score
Provides organization-specific risk-based impact score and prioritizes high-risk accounts for expedited incident response.

Indicators of Attack & Compromise
Leverage ML algorithms to search and identify suspicious activity such as pass-the-ticket or pass-the-hash and attempts to access and attack machines through M2M movement and automated scripts.

Time-series Analysis
Enables focus on specific timeframes to gain deeper insights into service account behavior and privilege spikes, reducing root-cause analysis time and expediting restoration.

94% of CISOs admit to not having full visibility into their service accounts. This creates a new gap in security, and puts organizations at risk for a privilege attack.

