Securing Service Accounts with Delinea's Secret Server

Delinea

Windows Service Accounts

How it works:

Secret Server discovers these accounts on Windows systems, manages their credentials, and rotates passwords automatically while updating dependent services to prevent disruptions.

Features used:

Discovery, Remote Password Changing (RPC), Heartbeat.

Business Driver & Value:

Reduces downtime and security risks from unmanaged credentials. Automating password rotation and dependency updates ensures uninterrupted service operations while mitigating the risk of breaches due to static, exposed credentials.

Active Directory (AD) Domain Accounts

How it works:

Integrates with AD to manage domain-level service accounts, rotating credentials and enforcing least privilege access across the domain.

Features used:

AD Integration, Password Rotation, Role-Based Access Control (RBAC).

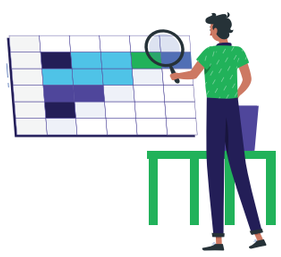
Business Driver & Value:

Enhances domain security and compliance. Centralized management and automated rotation reduce the attack surface in AD environments, critical for regulatory compliance (e.g., GDPR, HIPAA) and preventing lateral movement by attackers.

Local Windows Accounts

How it works:

Identifies local accounts on individual machines, rotates their passwords, and ensures compliance with security policies.



Features used:

Discovery, RPC, Auditing.

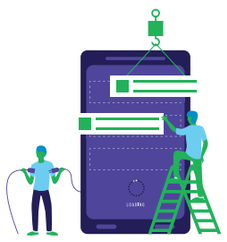
Business Driver & Value:

Mitigates risks from decentralized account management. Securing local accounts prevents unauthorized access on individual systems, supporting compliance and reducing insider threat risks.

Unix/Linux Service Accounts

How it works:

Manages accounts via SSH, rotating passwords and securing access to Unix/Linux systems hosting services or applications.



Features used:

SSH Key Management, RPC, Session Monitoring.

Business Driver & Value:

Strengthens security in heterogeneous environments. Automated credential management and session monitoring reduce vulnerabilities in Unix/Linux systems, critical for businesses with mixed infrastructures, ensuring operational continuity and auditability.

For more content like and follow me:  **@bertblevins**

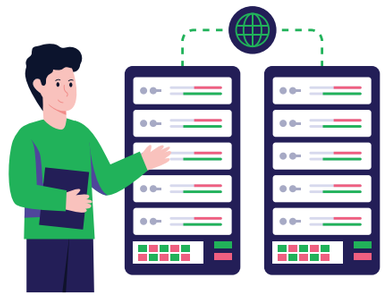
Securing Service Accounts with Delinea's Secret Server

Delinea

Database Service Accounts

How it works:

Connects to database systems to rotate credentials and restrict access, ensuring secure database operations.



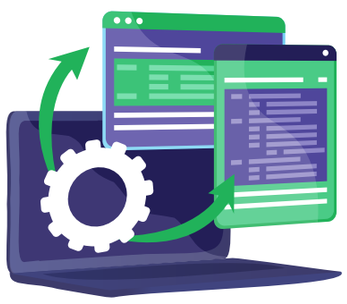
Features used:

Database Templates, RPC, Proxy (Session Control).

Business Driver & Value:

Protects sensitive data and ensures compliance. Securing database access prevents data breaches, a top business priority, while meeting stringent regulatory requirements (e.g., PCI DSS) through automated credential management.

Application Pool Accounts (IIS)



How it works:

Rotates credentials for IIS application pools and updates configurations to maintain uptime for web applications.

Features used:

Dependency Management, RPC, Heartbeat.

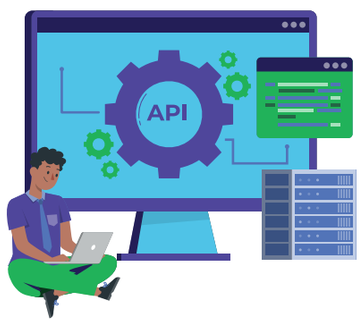
Business Driver & Value:

Ensures web application availability and security. Automating credential updates without downtime supports business-critical web services, reducing operational risks and enhancing customer trust.

Cloud Service Accounts

How it works:

Integrates with cloud provider APIs (e.g., AWS IAM, Azure Entra ID, GCP) to manage and rotate credentials for cloud-based services.



Features used:

Cloud Discovery, API Integration, Secret Vaulting.

Business Driver & Value:

Secures cloud adoption and scalability. Managing cloud credentials prevents misconfigurations—a leading cause of cloud breaches—enabling secure, compliant growth in cloud environments.

For more content like and follow me:  **@bertblevins**

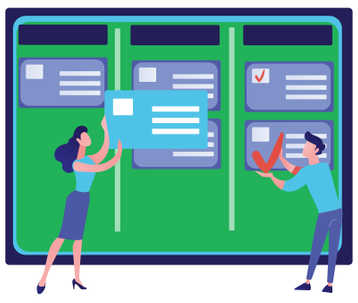
Securing Service Accounts with Delinea's Secret Server

Delinea

Scheduled Task Accounts

How it works:

Manages accounts tied to Windows Task Scheduler, rotating passwords and updating task definitions seamlessly.



Features used:

Dependency Management, RPC, Event Triggers.

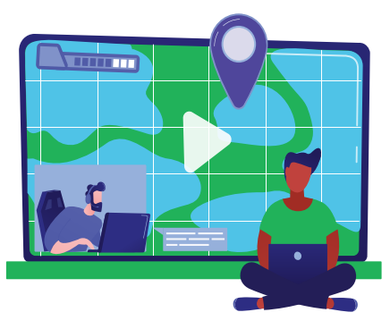
Business Driver & Value:

Maintains automation reliability and security. Ensures scheduled tasks run without interruption while securing credentials, critical for operational efficiency and reducing manual oversight costs.

Network Device Accounts

How it works:

Manages credentials for devices like routers and switches via SSH or Telnet, rotating passwords and securing access.



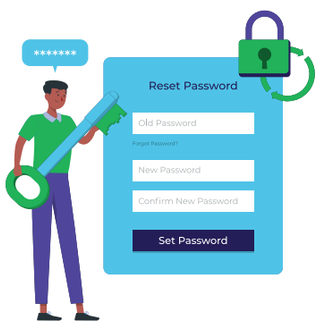
Features used:

Network Discovery, RPC, Session Recording.

Business Driver & Value:

Safeguards network integrity and uptime. Securing network devices prevents unauthorized access that could disrupt connectivity, ensuring business continuity and compliance with network security standards.

DevOps Service Accounts



How it works:

Secures accounts in CI/CD pipelines or automation tools by vaulting credentials and enabling secure API access.

Features used:

API Access, Secret Vaulting, Rotation Policies.

Business Driver & Value:

Accelerates secure DevOps workflows. Protecting credentials in fast-paced DevOps environments reduces security bottlenecks, enabling faster delivery while maintaining robust security posture.

For more content like and follow me:  **@bertblevins**

Securing Service Accounts with Delinea's Secret Server

Delinea

VMware ESX/ESXi Accounts

How it works:

Manages credentials for VMware virtualization hosts, rotating passwords and ensuring secure access to ESX/ESXi systems.

Features used:

Discovery, RPC, Auditing.

Business Driver & Value:

Enhances virtual infrastructure security. Securing virtualization layers prevents breaches that could compromise entire data centers, supporting reliable, compliant virtualization strategies.

Custom Service Accounts

How it works:

Allows tailored management for unique applications or scripts, rotating credentials and updating dependencies as defined by custom scripts or templates.

Features used:

Custom Templates, Scripting (PowerShell/SSH), Dependency Management.

Business Driver & Value:

Provides flexibility for unique business needs. Customizable management ensures security for proprietary systems, reducing risks in specialized environments and aligning with specific operational requirements.

Overall Business Value of Delinea Secret Server

Delinea Secret Server adds value by addressing key business drivers such as security, compliance, operational efficiency, and scalability. It reduces the risk of credential-based attacks (a common entry point for breaches), ensures adherence to regulatory standards, minimizes manual IT overhead through automation, and adapts to diverse and evolving IT landscapes.

By centralizing and automating privileged account management, it empowers organizations to protect critical assets, maintain service availability, and support digital transformation—all while reducing costs and complexity associated with manual processes.

For more content like and follow me:  **@bertblevins**