Secure DevOps

Integrated Vulnerability Management, Secrets Management & Privilege Management

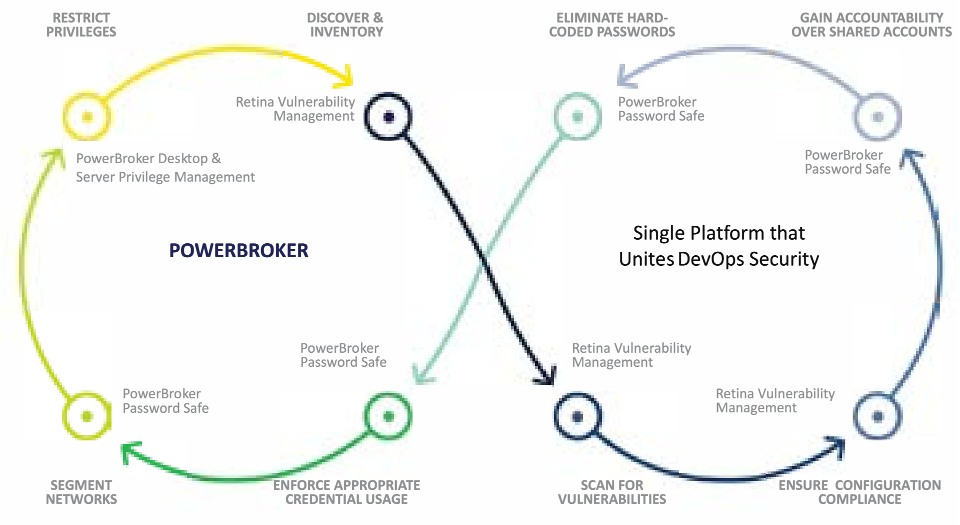
While DevOps promises better products and condensed release cycles, security and compliance across these environments can't be an afterthought. Consider the DevOps security risks:

- Malicious insiders can leverage excessive privileges or shared secrets to compromise code
- Vulnerabilities, misconfigurations, and other weaknesses in containers can open the door to security compromises
- Insecure code, hard-coded passwords, and other privilege exposures can lead to external attacks
- Scripts or vulnerabilities in CI/CD tools – such as Ansible, Chef, or Puppet – could deploy malware or sabotage code

While it's clear that security needs to be built into DevOps, how do you do so without hampering speed and agility?

Enable Secure DevOps for Business Agility

The BeyondTrust solution for enabling secure DevOps reduces risks throughout the IT supply chain by improving visibility and control over secrets, admin privileges, and system configurations and vulnerabilities. By uniting these capabilities across on-prem, virtual, cloud, and DevOps use cases, IT organizations can achieve their agility goals without burdensome processes.


RESTRICT PRIVILEGES
DISCOVER & INVENTORY
ELIMINATE HARD-CODED PASSWORDS
GAIN ACCOUNTABILITY OVER SHARED ACCOUNTS
Retina Vulnerability Management
PowerBroker Password Safe
PowerBroker Desktop & Server Privilege Management
PowerBroker Password Safe
POWERBROKER
Single Platform that Unites DevOps Security
PowerBroker Password Safe
Retina Vulnerability Management
PowerBroker Password Safe
Retina Vulnerability Management
SEGMENT NETWORKS
ENFORCE APPROPRIATE CREDENTIAL USAGE
SCAN FOR VULNERABILITIES
ENSURE CONFIGURATION COMPLIANCE

BeyondTrust features an 8-step best practices framework for enabling secure DevOps for business agility.

Key Capabilities

- Inventories all DevOps assets
- Scans for vulnerabilities and configurations across dev, test and production systems
- Finds and controls the use of all hard-coded passwords and shared secrets
- Eliminates excessive privileges on developer machines
- Enforces boundaries between dev, test and production systems
- Unites all features into a single platform for management

Key Benefits

- Ensures that only properly configured and approved images are used in your environment
- Improves visibility by providing continuous vulnerability assessment and remediation guidance across physical, virtual and, cloud environments
- Improves accountability by ensuring that all secrets are properly managed and rotated, and that all audited activity is associated with a unique identity
- Reduces risk by restricting developer/tester access to development, management and production systems, limiting lateral movement
- Maintains agility and productivity by integrating with tools and processes already in place

The PowerBroker Privileged Access Management Platform

BeyondTrust solutions for DevOps are part of the PowerBroker Privileged Access Management Platform, which delivers visibility and control over all privileged accounts, users. and assets. The platform integrates a comprehensive set of PAM capabilities across on-prem, virtual, and cloud to simplify deployments, reduce costs, improve system security, and reduce privilege-related risks. PowerBroker solutions include:

- **Enterprise Password Security:** Provide accountability and control over privileged credentials and sessions
- **Server & Infrastructure Privilege Management:** Control, audit, and simplify access to DevOps systems
- **Endpoint Privilege Management:** Remove excessive user privileges and control applications on endpoints

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

LATAM
latam@beyondtrust.com

CONNECT

Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

Key Features

Discovery & Inventory: Performs continuous discovery and inventory of container instances, libraries, and more across physical, virtual, and cloud environments.

Vulnerability Scanning: Scans container instances and libraries, with options for offline image scanning, start/stop image scanning, and image integrity tracking.

Configuration Compliance Scanning: Performs continuous configuration and baseline scanning against industry configuration guidelines and best practices from NIST, STIGS, USGCB, CIS, and Microsoft, across servers and code/builds in physical, virtual, and cloud-deployed assets.

Shared Secrets Management: Controls and audits access to shared secrets, including developer access to source code, DevOps tools, test servers, and production builds.

Eliminate Hard-Coded Credentials: Controls access to scripts, files, code, embedded application credentials, and hard-coded passwords, including removing hard-coded passwords in DevOps tool configurations, build scripts, code files, test builds, and production builds.

Enforce Appropriate Credential Usage: Eliminates administrator privileges on end-user machines, securely stores privileged account credentials, requires a simple workflow process for check-out, and monitors privileged sessions.

Segment Networks: Utilizes a secured jump server with multi-factor authentication, adaptive access authorization, and session monitoring for access that needs to cross trust zones.

Restrict Privileges: Grants only required permissions to appropriately build machines and images, and deploy, configure, and remediate production issues on machines and images.