PowerBroker for Networks

Network Device Privilege Management

BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

The current security landscape requires organizations to have granular control and detailed auditing of activities that occur on networks. Some network devices – like routers, switches, and firewalls – present a challenge to using traditional agent based solutions to provide the level of auditing and control desired. These devices provide critical functions and are often-overlooked targets for external attackers and malicious insiders. When managing a heterogenous network of devices it is difficult to find a single solution to provide a consistent level of policy controls and auditing of your infrastructure. Best practices recommend that passwords to these devices are securely stored and regularly changed, but enterprise password management addresses only part of the problem.

- What happens after the user logs on to the device?
- Can you control what commands are being run?
- Can the session be recorded?
- Can active sessions be viewed, paused and terminated?
- Is audit data centralized and indexed?

Simple command blacklisting doesn't offer enough granularity to prevent unwanted commands from being run. There are only a very limited number of tools on the market to help secure network devices. Most have minimal functionality and work only on a limited number of devices. How can security and IT teams achieve granular command control and full auditability on network devices to prevent cyber attacks?

Command Control and Session Auditing without Agents

PowerBroker for Networks is a privilege management solution that secures access to network devices, enabling organizations of all sizes to reduce cybersecurity risk and achieve privilege management at scale. PowerBroker provides IT organizations with flexibility to control:

- Who is allowed to run a command on a device
- What commands and arguments can be passed to a target device
- Where is an authorized command allowed to run
- When during the day, week or month is a command allowed to run

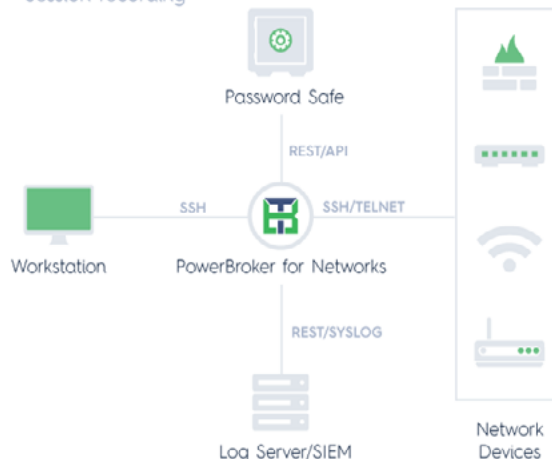DIRECT ACCESS WITHOUT
PowerBroker for Networks
· Unfettered access
· Little or no audit

DIRECT ACCESS WITH
PowerBroker for Networks
· Command Control (Full Policy Based Control)
· Auditing (Eventlog, Syslog and Alerting)
· Session recording

Solution Overview

FULL COMMAND CONTROL AND SESSION AUDITING

Enable full, granular control and audit of all commands and sessions to network devices.

REAL-TIME SESSION MONITORING

Warn, or warn then terminate, a session when questionable user behavior is detected.

INTEGRATE WITH SIEM SOLUTIONS FOR COMPLETE SECURITY INTELLIGENCE

Generate logs and send to syslog to be picked up by a SIEM system.

ALERTING FOR FASTER CYBERSECURITY RESPONSE

Generate alerts to prevent, or stop, unwanted activity.

AUTOMATE SINGLE SIGN-ON

Integrate with password management solutions to seamlessly retrieve passwords for automated sign-on through a proxied connection.

PRIVILEGE MANAGEMENT AT SCALE

Modular design is highly scalable, allowing one to hundreds of thousands of managed nodes, delivering optimal performance without limiting activity through a proxy or central gateway.

CENTRALIZED CONTROL

Centralized administration, policy and audit data for decentralized devices and administrators.

The PowerBroker Privileged Access Management Platform

PowerBroker for Networks is part of the BeyondTrust 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 to simplify deployments, reduce costs, improve system security, and reduce privilege-related risks. Solutions include:

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

CONTACT

North America
info@beyondtrust.com

EMEA
emeainfo@beyondtrust.com

APAC
apacinfo@beyondtrust.com

CONNECT

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

Policies can be simple, such as a basic list of users coupled with allowed commands, or can be driven by external data sources such as reference files, databases, or LDAP queries that allow for powerful command validation and dynamic rules to be created, ultimately providing total flexibility and granularity over each user's session.

Key Security Features

- **Full command control:** Enable full, granular control of all commands run on network devices.
- **Audit and session recordings:** Audit all commands and sessions to network devices, ensuring enhanced security.
- **Flexible policy language:** Highly granular policy language ensures superior control over all commands entered, as opposed to what simple blacklisting offers.
- **Data-driven policy:** Make decisions to accept/reject/alter commands based on external data sources, such as databases or LDAP query.
- **Command alteration:** Manipulate all, or part, of a command that gets sent to the target device.
- **Session termination:** Terminate a user's session based on questionable commands, or repeated bad behavior, to stop potential harmful activity in its tracks.
- **Syslog support:** PowerBroker has the ability to send selective, or all actions, to syslog, allowing SIEM systems to build a complete picture of user activity.
- **Whitelist/blacklist capability:** Default behavior of accepting commands or rejecting commands allows PowerBroker to run in either a blacklist or whitelist mode.
- **Customize end user messaging:** Prompt users, detect logins, offer a message of the day, or send warnings or one-time messages to users based on commands.

Key Automation Capabilities

- **Automated single sign-on (SSO):** Built-in integration with PowerBroker Password Safe allows administrators to seamlessly retrieve passwords, enabling automated sign-on through a proxied connection. Also supports other major password management systems.
- **Automate repetitive tasks:** PowerBroker automates repetitive tasks, including actions at logon.
- **Multiple actions per command:** PowerBroker enables a user to type a single command to execute any number of other commands, improving efficiency.
- **Include external data files:** Break policy into multiple files for easier administration.
- **REST Interface:** PowerBroker offers a HTTP-based API to administer policies via web services.
- **Tab and line completion:** PowerBroker automatically completes commands and entire lines.

Supported Platforms

PowerBroker supports any SSH or Telnet device, with full command control and auditing.