BlackRidge TECHNOLOGY

Insider and Third Party Protection Datasheet

Solution Overview

Objective

Control insider and third party vendor access to and visibility of servers. Stop unauthorized access, and provide user attribution to detect insider threats. Demonstrate audit and compliance controls and reporting.

Capabilities

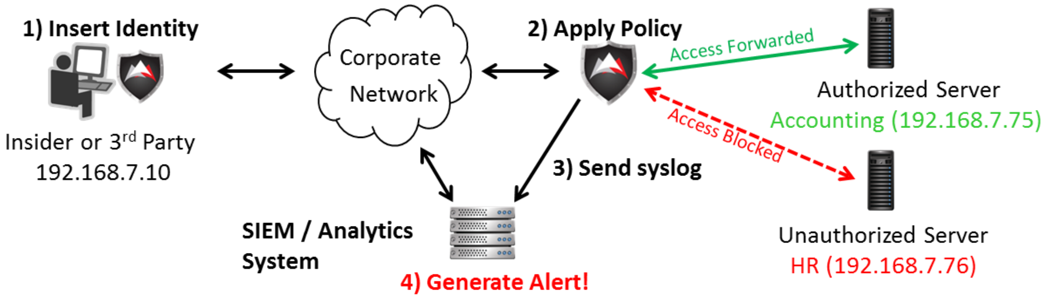
- **Authenticates access** to servers prior to a network connection, the earliest possible time, using existing identity of insiders and third party vendors and partners.
- **Real time logs** of all identified and unauthorized connection attempts with identity attribution to a security event management or analytics system for forensic analysis.
- **Generate alerts** from security event management and analytics systems of unauthorized access attempts with user or device identity attribution.

Benefits

- **Prevents unauthorized access** to data and contains breaches from spreading across internal systems or a partner's network and systems.
- **Limits risk** from third partner vendors and partners on your network by implementing a least privilege model with attribution information for compliance and forensics.
- **Proof of controls** to compliance auditors and regulators; Enables IT to handle exceptions.

Solution Workflow

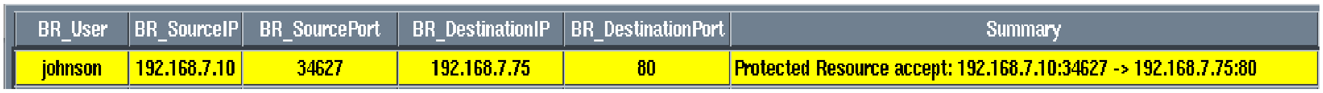
A third party vendor access policy is configured in BlackRidge to allow access to only specific servers for the vendor. BlackRidge is configured to dynamically learn identities from the corporate Identity Management System when a user logs in. A BlackRidge virtual or physical appliance at the network access point or on the user system inserts identity into TCP/IP sessions, and a downstream BlackRidge appliance authenticates the identity and allows or denies access to protected server resources.



Authorized Server Access Workflow

Third party user Johnson logs in to a local system and attempts to access data or an application on an authorized and protected server Accounting (192.168.7.75):

1) **Insert Identity:** Identity is transparently inserted into connection attempt to Accounting.
2) **Apply Policy**: User connection attempt is received across the network, the user identity is authenticated, and the connection setup attempt is Forwarded to the Accounting server.
3) **Send Syslogs:** Attribution for an authorized action is sent to the SIEM or analytics system.



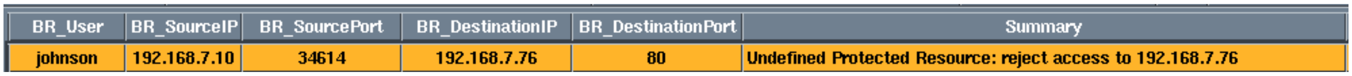
BR_User	BR_SourceIP	BR_SourcePort	BR_DestinationIP	BR_DestinationPort	Summary
johnson	192.168.7.10	34627	192.168.7.75	80	Protected Resource accept: 192.168.7.10:34627 -> 192.168.7.75:80

4) **No alert** is generated and the events are recorded for compliance and forensic analysis.

Unauthorized Server Access Workflow

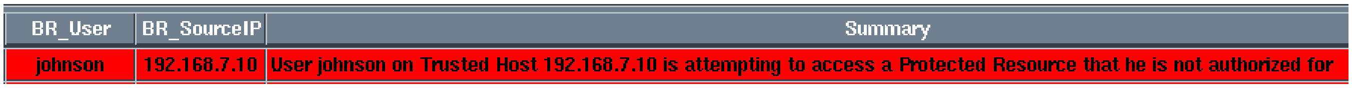
Third party user Johnson logs in to a local system and attempts to access an application on an unauthorized and protected sever, HR (192.168.7.76).

1) **Insert Identity:** Identity is transparently inserted to a connection attempt to HR server.
2) **Apply Policy**: User connection attempt is received across the network, the user identity is authenticated, and the connection setup attempt is Blocked with no response.
3) **Send Syslogs:** User attribution for an unauthorized action is sent to SIEM or analytics system.



BR_User	BR_SourceIP	BR_SourcePort	BR_DestinationIP	BR_DestinationPort	Summary
johnson	192.168.7.10	34614	192.168.7.76	80	Undefined Protected Resource: reject access to 192.168.7.76

4) **Generate Alert:** The SIEM or analytics system generates an alert and records the events for compliance and forensic analysis.



BR_User	BR_SourceIP	Summary
johnson	192.168.7.10	User johnson on Trusted Host 192.168.7.10 is attempting to access a Protected Resource that he is not authorized for

5) **Take Action:** Security/IT can act on the alert with the user identity attribution information to disable or reduce permissions of the rouge user in the identity management system (IDMS), or directly in the BlackRidge system. A change to the user's privileges in the IDMS is detected and the corresponding actions are taken in BlackRidge, including a policy update or removal of the dynamic identity.

Solution Summary

BlackRidge provides an identity-based solution for controlling insider and third party vendor access to and visibility of servers. Real-time user attribution information is provided to enable alerts from security event management and analytics systems of unauthorized access attempts, with user or device identity attribution. This enables compromised identities to be flagged and it supports audit and compliance controls and reporting.

Identity-based network protection provides a practical way to describe and monitor access policies, handle exceptions, and provide proof to auditors and regulators of your controls including who is doing what. Full transparency is provided by simply monitoring access exceptions at the network layer, and providing attribution information to your policy and procedures teams for reporting and remediation.

About BlackRidge Technology

BlackRidge Technology provides a next generation cyber defense solution that stops cyber-attacks and blocks unauthenticated access. BlackRidge Transport Access Control authenticates identity and enforces security policy on the first packet of network sessions, providing a new level of real-time cyber defense that isolates and cloaks servers and clouds and segments networks.