BlackRidge TECHNOLOGY

Identity-Based Network and Cyber Defense

Only Cyber Defense Solution that Stops Unknown Attacks and Protects Against Insider Threats

Next Generation Solution

BlackRidge Technology provides next generation cyber defense that stops cyber-attacks and blocks unauthenticated access by isolating and cloaking servers and clouds, segmenting networks, and providing identity attribution.

Developed for the military, BlackRidge authenticates identity and applies security policy on the first packet of network sessions, the earliest possible time to engage. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic including port scanning and reconnaissance. This greatly reduces risk, simplifies compliance, and increases operational efficiency by eliminating unauthorized traffic from networks and servers.

Cloaked and Protected

End-to-End Solution

The BlackRidge identity-based model for network security operates end-to-end across network boundaries with multiple policy enforcement points, without impacting network compatibility. BlackRidge provides high throughput and low latency network security that operates pre-session, in real time, before next generation firewall and application security defenses engage.

BlackRidge uses a highly scalable, non-interactive authentication protocol that does not rely on signatures, sandboxing, or deep packet inspection. Operating at the Transport Layer, BlackRidge is compatible with existing network and security technologies and middle boxes, it is address and topology independent, and supports it NAT.

How it Works

BlackRidge Transport Access Control (TAC) performs identity insertion, resolution and policy enforcement for network sessions. TAC inserts a cryptographically secure, single-use identity token into a TCP/IP session into the first packet of a TCP connection request. When the connection request is received on the server side, TAC extracts and authenticates the identity and applies a security policy — forward, redirect, or discard the connection request — based on the identity.

Identity can be provisioned through the BlackRidge Enterprise Manager and securely provisioned with amongst BlackRidge gateways and endpoints. or dynamically learned via an integration with an identity management system. The latter occurs when a user or device authenticates with an IDMS such as Microsoft Active Directory®. This allows enterprises to implement security policy using existing identity associations, vs. using router ACLs and firewall policies that depend on network topology and addresses that are not authenticatable or secure.

Log records are generated for each policy action, providing real-time information on unidentified and unauthorized access for early detection of insider or third party incidents and or compliance reporting.

Key Deployment Use Cases

Easy to Deploy and Maintain

The BlackRidge solution is easy to deploy and maintain since it operates in a "set it and forget it" mode in a variety of network, virtual server and cloud configurations. The BlackRidge solution can be flexibly deployed as physical appliances or virtual network or cloud appliances and soon as software endpoints.

BlackRidge can be deployed in front of existing security stacks to block or filter anonymous traffic or placed inside the network to isolate and protect servers or segment networks.

Isolate and Protect Services

BlackRidge TAC provides a new level of cyber defense to isolate and protect critical services and provide access attribution across enterprises and hybrid clouds. As depicted on the right, BlackRidge gateways are placed between an access network or campus and the servers, enclaves, or datacenters to be segmented and protected.

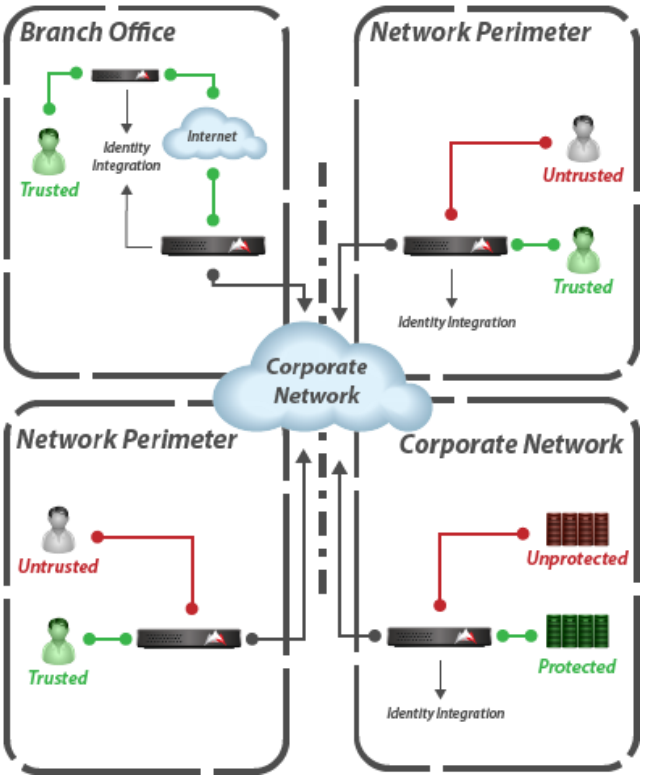
Network Segmentation

Network segmentation is a security and compliance best practice that is increasingly impractical to maintain in enterprise and cloud environments. The traditional approaches of maintaining ACLs and firewall rules has high administrative overhead and network topology dependencies. Using firewalls for interior network segmentation can be costly and impact application performance.

BlackRidge provides a new software-based approach to segmentation with identity-based access controls to block or allow network connections. This provides granular security zones on shared networks without creating separate physical or logical networks.

Protect Remote Offices

BlackRidge extends identity across Virtual Private Network (VPN) and network boundaries



and applies policy (forward, drop, or redirect) at multiple enforcement points. This end-to-end security architecture reduces risks from remote and branch office access into corporate networks while increasing your security and compliance posture.

Isolate Management and Control Networks

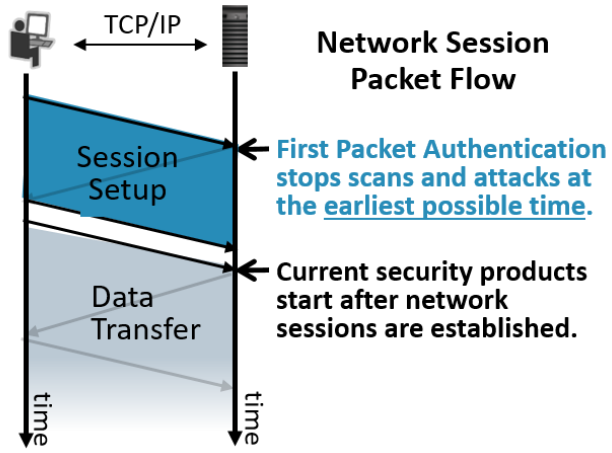
Management and control networks are the foundation upon which business systems are built. They need to be further protected from cyber-attacks and insider threats, including privileged account and third party risks.

BlackRidge TAC isolates and protects IT management networks, control planes and management systems from unauthorized users and devices. This additional layer of protection lowers risks of IT management systems being attacked and provides identity attribution information for each network session.

Unique Differentiators

First Packet Authentication™

BlackRidge TAC authenticates identity and applies security policy on the first packet of network sessions. A cryptographic single-use identity token is inserted into the first TCP packet that is then recognized and resolved to authenticate the identity of the TCP connection requestor. Security policy is then enforced to forward traffic to authorized resources, or block or redirect unauthorized and anonymous traffic with no response. First Packet Authentication provides low and deterministic latency — no deep packet or content inspection is required.



Dynamic Identity Integration

BlackRidge TAC integrates with Microsoft Active Directory and other identity management systems to dynamically learn user and device identities, and simplify configuration of policy for accessing resources. BlackRidge gateways can also be configured with static identities.

Automated Identity and Policy Deployment

BlackRidge TAC securely and automatically distributes and manages session keys for identity tokens. This occurs securely and transparently between TAC gateways and requires no additional management or action by IT or security administrators. This simplifies management processes and eliminates risk and complexity of maintaining stored keys.

Blocks Network Scanning and Reconnaissance

BlackRidge blocks all network and server scanning and reconnaissance from unidentified and unauthorized users. Blocking scanning and effectively stops attackers in their tracks - you can't attack what you can't see.

This greatly lowers the risk of key servers being compromised and it provides attribution information for compliance about who is attempting to access the servers.

BlackRidge blocks scans down to a single packet probe effectively cloaking the protected network or server resource. This includes "low and slow" scans that avoid traditional heuristic and rate based detection approaches.

End-to-End Protection

BlackRidge provides a new level of network and cyber security protection from all access points throughout the enterprise or hybrid cloud. BlackRidge works across LAN and router boundaries and automatically adjusts to changing network topologies, ensuring that systems are secure end-to-end.

Identity Attribution

Authentication of TCP/IP sessions enables TAC to provide identity attribution along with the TCP/IP session information to Security Information and Event Management (SIEM) and analytics systems. This is the earliest possible time that attribution information can be provided to the analytics system. Identity attribution information is higher quality that tradition TCP/IP session information alone, since addresses in TCP/IP sessions can be easily spoofed and should not be used authoritatively for security policy.

BlackRidge TAC Features

Gateway Features

- TCP Identity Token Insertion and Resolution
- First Packet Authentication
- Adjustable Confidence Thresholds
- Dynamic Identity for Users/Devices
- Static Identity for Users/Devices
- Microsoft Active Directory Integration
- Protected Resource Groups
- Unprotected Resource Table
- Traffic Policy - Forward/Drop/NAT
- Traffic Policy - Layer 4 Application Ports
- Policy Action Logging with Identity Attribution
- Adaptive Nulling / Dynamic Blacklisting
- 1GbE Desktop and 1GbE/10GbE Network Appliances
- AWS, IBM z Systems, and VMware Virtual Appliances
- Syslog messages for SIEM integrations

Gateway Modes of Operations

- Bridge Mode
- Policy Monitor Mode
- Policy Enforce Mode
- Layer 2 Transparent Mode
- Layer 3 NAT Mode

Gateway Management

- Command Line and Console Access
- Web-based Graphical User Interface
- Enterprise Management System
- Integrated Database
- PKI Identity Support
- REST APIs

Enterprise Gateways

Cloud and Virtual Appliances

Branch/Desktop Gateways

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, segments networks, and provides identity attribution.