Micro-Segment Networks, Isolate Cloud Services, and Cloak and Protect Servers

Adaptive Cyber Defense

Enterprises and service providers need to deliver more secure and resilient business services in today's rapidly evolving technology, computing and cyber threat environments. This need can be addressed by implementing adaptive security models that prevent known and unknown attacks, rather than simply detecting and reacting to attacks once networks and sensitive data have already been breached.

Developed for the US Department of Defense, BlackRidge Technology products provide an adaptive cyber defense solution that proactively isolates cloud services, cloaks and protects servers and segments networks**.** This new level of real-time protection blocks or redirects unidentified and unauthorized traffic to stop cyber-attacks and unauthorized access, including port scanning and reconnaissance. This greatly reduces risk, simplifies compliance, and increases operational efficiency by eliminating unauthorized traffic from networks and servers.

End-to-End Solution

The BlackRidge identity-based, adaptive trust model for network security operates end-to-end across network and cloud boundaries with multiple policy enforcement points, without impacting network compatibility. This 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, is address and topology independent, and supports Network Address Translation (NAT).

How it Works

BlackRidge software products take a patented approach to authenticating network sessions, called First Packet Authentication™. Transport Control Protocol (TCP), the Internet protocol used to connect to servers, does not allow identity credentials to be exchanged until after a network session is fully established. This widely exploited design flaw exposes critical resources to attack from the Internet. You can't know whom your network is "talking to" until the conversation is under way.

BlackRidge Transport Access Control (TAC) enhances TCP to close this vulnerability by using cryptographically secure, single-use identity tokens to authenticate TCP/IP requests *before* a session is established. No conversation takes place until TAC software authenticates the identity token and applies a security policy — forward (with NAT or QOS classification) or drop — to the connection request. In this way, TAC cloaks and protects network resources from network reconnaissance, port scans and many other forms of unauthorized access. Your network is a "black hole," emitting no information of any kind (not even a SYN/ACK packet) until the right to communicate with network resources is established.

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

Key Deployment Use Cases

Micro-Segmentation

Network or micro-segmentation is a security and compliance best practice that is difficult and costly to implement with traditional approaches of maintaining ACLs and firewall rules. Firewalls have high administrative overhead, network topology dependencies, and for datacenter interior network segmentation they are 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 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.

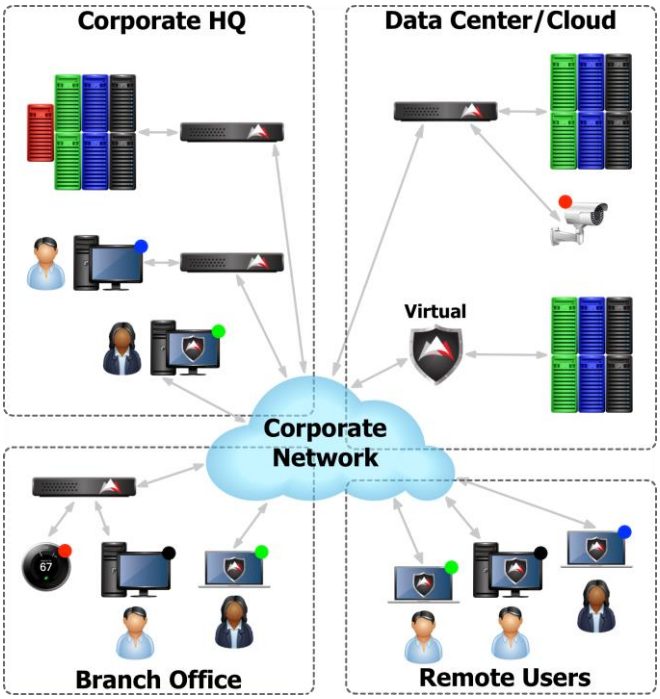
BlackRidge TAC isolates and protects IT management networks, control planes and management systems from unauthorized users and devices. This additional layer of protection lowers risks of IT management systems being attacked and provides identity attribution information for each network session.

Cloak and Protect Servers

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.

Software Defined Perimeter

BlackRidge TAC extends identity across Virtual Private Network (VPN) and network boundaries and applies policy at multiple enforcement points. This end-to-end security architecture reduces risks from remote and branch office access into corporate networks or to cloud services, while increasing your security and compliance posture. Distributed cloud services like blockchain can be protected from unauthorized access and DDoS attacks.



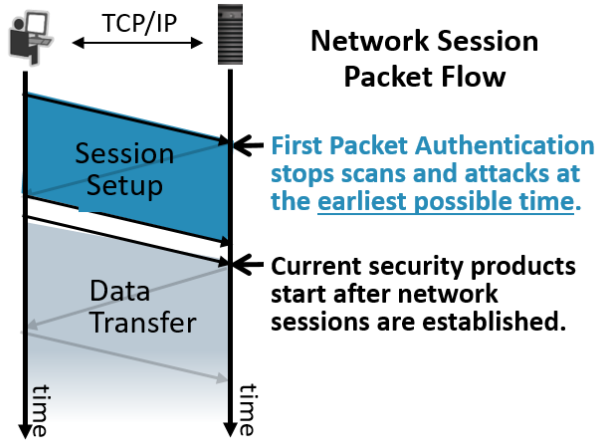
Protect ICS and IIoT Systems

The BlackRidge approach to micro-segmentation and isolation provides many advantages for Industrial Control Systems (ICS) and the Industrial Internet of Things (IIoT) including infrastructure and topology independence that is multi-vendor and heterogeneous. BlackRidge TAC can be integrated into ICS controllers and devices, deployed at the edge in gateways, and it supports legacy brownfield environments.

Unique Capabilities and 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 packet of a TCP session. The token is then resolved to authenticate the identity of the TCP connection requestor and apply security policy — forward (with NAT or QOS classification) or drop — to the connection request. 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 and can map identity to an IP or MAC address.

Easy to Deploy and Maintain

BlackRidge TAC operates in a "set it and forget it" mode. TAC gateways securely distribute and transparently manage session keys for identity tokens. No additional management or action is required by IT or security staff. This simplifies management processes and eliminates the risk and complexity of maintaining stored keys. The BlackRidge solution can be flexibly deployed as physical appliances, virtual or cloud appliances and as software endpoints, both inside and outside the corporate network or in private and public clouds.

Blocks Network Scanning

BlackRidge TAC blocks all network and server scanning and reconnaissance from unidentified and unauthorized users. Blocking port scanning effectively stops attackers in their tracks — you can't attack what you can't see — effectively cloaking the protected network or server resource. This includes "low and slow" scans that avoid traditional detection approaches. This greatly lowers the risk of key servers and network equipment being compromised.

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 sessions enables TAC to log identity attribution with session information to security event management and analytics systems. This is the earliest possible time that attribution information can be provided, and it is higher quality than session information alone, since addresses can be easily spoofed and should not be used authoritatively for security policy.

Trust Level Feedback Policy

BlackRidge enables external analytics systems and administrators to adaptively adjust the trust level of individual identities. Trust policies are defined on a system wide or per identity group basis. This additional level of adaptive security enhances protection in response to events to ensure resources remain protected.

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 (with NAT or QOS classification) or Drop
- Traffic Policy - Layer 4 Application Ports
- Trust Level Policy
- Trust Feedback API
- TCP Session ID (SID) Tagging
- Policy Logging with Identity Attribution
- Adaptive Nulling / Dynamic Blacklisting
- Syslog messages for SIEM integrations
- VLAN support
- FIPS 140-2 Level 1 Validation

Platforms Supported

- Windows 7/10, Ubuntu Linux endpoints
- 1GbE desktop appliance
- 1GbE/10GbE network appliances
- AWS, IBM z/VM®, KVM, and VMware appliances

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 Management Counsel
- BlackRidge Enterprise Manager
- Integrated Database
- REST APIs
- NIST 800-53 Access Control Features

Enterprise Gateways

Cloud and Virtual Gateways

Branch/Desktop Gateway

Software Endpoints

About BlackRidge Technology

BlackRidge Technology provides an adaptive cyber defense solution that enables our customers to deliver more secure and resilient business services in today's rapidly evolving technology and cyber threat environments. The BlackRidge Adaptive Trust solution provides end-to-end security that proactively isolates cloud services, protects servers and segments networks**.** Our patented First Packet Authentication™ technology authenticates user and device identity and enforces security policy on the first packet of network sessions. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic to stop cyber-attacks and unauthorized access.