Network Security and Cyber Defense for IBM z Systems

Identity-Based Network Security and Cyber Defense

BlackRidge Technology provides a new layer of cyber security defense to protect against today's advanced cyber-attacks and insider and third-party threats. This additional layer of military proven protection is available for IBM z Systems™ to help clients take advantage of the cloud while ensuring their distributed systems are secure end-to-end in enterprise and hybrid cloud environments. BlackRidge network security protection is additive to z Systems security offerings and it provides real-time attribution with identity to IBM QRadar® and analytics systems.

BlackRidge authenticates user or device identity and applies policy at the earliest possible time for security defenses to engage—on the first packet of a network session. The BlackRidge Gateway for z Systems is a software appliance solution that has achieved the **Ready for IBM Security Intelligence for z Systems** validation.

Business Partner IBM
Ready for Security Intelligence

Designed to further protect IBM z Systems and IBM LinuxONE™ workloads and to protect distributed enterprise and hybrid cloud deployments, the key use cases for deploying BlackRidge include:

- Real-time protection from insider threats and outside network-based attacks
  - Authenticates TCP connections to allow only authorized access to a mainframe
  - Protects and isolates workloads within a mainframe allowing only authorized access
  - Protects distributed application server and B2B partner network access
- Protect distributed and cloud applications on IBM z Systems
  - Stops scanning and reconnaissance - ports cannot be found
  - Minimizes attack surface - you can't attack what you can't see
  - Allows only identified and authorized users/devices network access to applications
- Segment and isolate workloads to reduce risk and meet compliance
  - Identity-based segmentation to meet network compliance objectives
  - Real-time logs with identity attribution to QRadar/SIEM and analytics systems
  - High throughput, low latency for minimal performance impact (no content inspection)

BlackRidge Gateway for z Systems

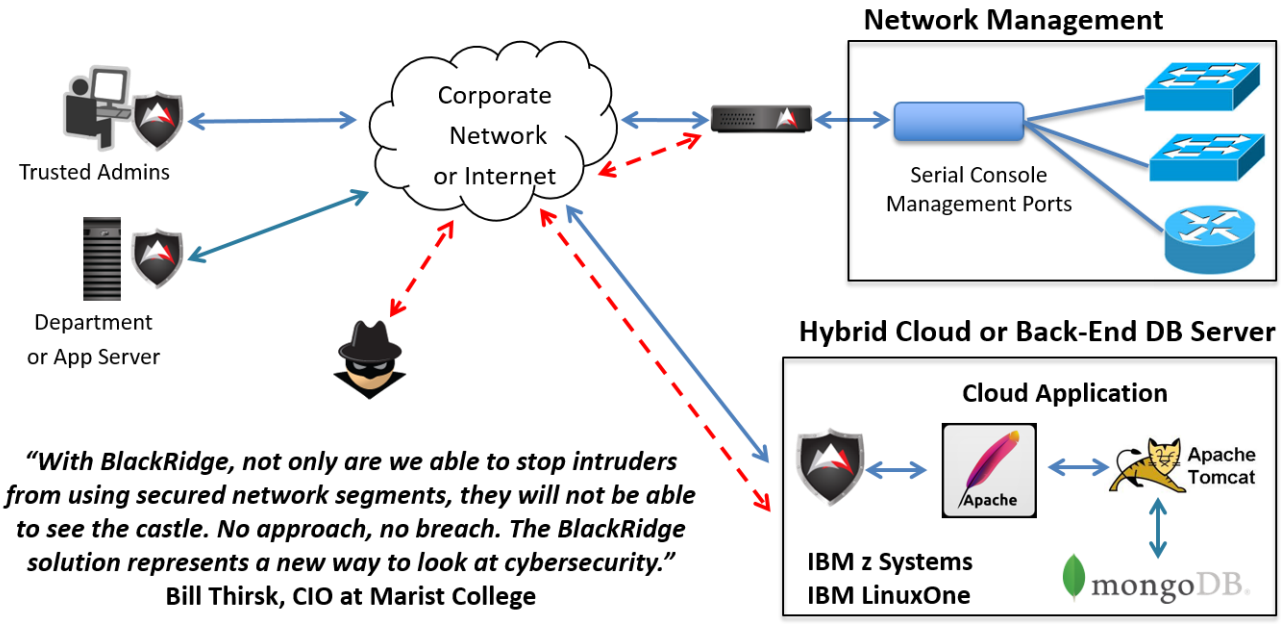
The BlackRidge Gateway for z Systems is a self-contained, easy to deploy software appliance that runs on an IBM z System IFL (Integrated Facility for Linux), a processor dedicated to running Linux workloads, or alternatively as a guest on z/VM®.

The BlackRidge gateway can be used to protect any z Systems workloads regardless of the operating system being used (e.g. z/OS, z/Linux, VSE, z/VM, and z/TPF). The BlackRidge gateway isolates networked workloads and administrative portals from potential attacks from unauthorized internal users or from untrusted external devices. Individual engines can be isolated from other z Systems resource access or traffic, essentially segmenting key applications or departmental assets for compliance.

BlackRidge software and systems are designed to be highly resilient and can be configured for high availability and failover. Security policies can be verified during deployment to ensure correct operation with progressive policy enforcement operational modes of bridge, monitor, and then enforce mode.

Example Use Cases

Two use cases are depicted below for protecting the management interfaces of a production network and protecting critical business servers and sensitive data in a cloud or a back-end database server. Management networks are the foundation upon which business systems are built and they need to be further protected from cyber-attacks and insider threats, including privileged account and 3rd party risks. Key servers and sensitive data likewise needs to be protected from unauthorized network access and segmented for compliance.



"With BlackRidge, not only are we able to stop intruders from using secured network segments, they will not be able to see the castle. No approach, no breach. The BlackRidge solution represents a new way to look at cybersecurity."
Bill Thirsk, CIO at Marist College

The trusted users and servers accessing the protected resources are shown on the left where BlackRidge inserts an identity token into the first packet of the network connection request to the critical resource. On the resource side, BlackRidge authenticates the identity and applies the security access policy for the user or device attempting the connection. Unidentified or unauthorized access attempts to the protected resource are either blocked or redirected with no response back. The policy action is then logged for monitoring, compliance or forensic purposes.

BlackRidge can be deployed as a network gateway in front of protected resources as shown for the management of the production network, or as a software appliance as shown for the IBM z Systems cloud or database server.

About BlackRidge

BlackRidge Technology provides a next generation cyber defense solution that stops cyber-attacks and blocks unauthenticated access. Our patented First Packet Authentication™ technology was developed for the military to cloak and protect servers and segment networks. BlackRidge Transport Access Control 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 attacks and unauthorized access, isolates systems and segments networks, and provides identity attribution. BlackRidge was founded in 2010 to commercialize its military grade and patented network security technology.