Enterprise Plus Security for Cisco Environments

BlackRidge TECHNOLOGY

Extending Cisco Identity Services Engine (ISE) to Protect Critical Enterprise Assets

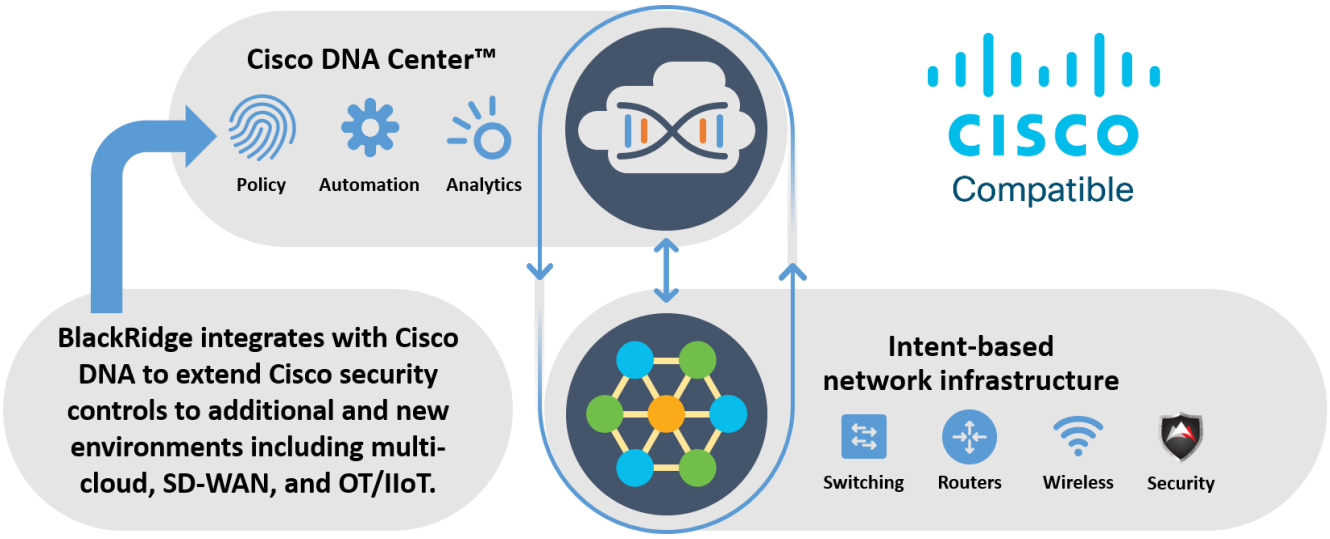
BlackRidge Technology has partnered with Cisco to solve the inherent security problems — and lessen the resulting business impact — of enterprise networks that allow user and device traffic onto networks before their identity is authenticated. Business risk continues to grow with the increasing attack surface represented by the introduction of multi-cloud systems and their integration with enterprise systems, and more recently by the convergence of operational technology (OT) systems and devices with information technology (IT) networks.

Cisco Partner
Solution Partner

BlackRidge implements a zero-trust network connection model by authenticating identity and applying security policy before allowing network connections to be established, independent of network topology. This gives enterprises the ability to segment and isolate key systems, applications and resources from unauthorized access while also identifying, tracking and acting on each connection attempt.

Enterprise Plus Security

The BlackRidge solution for Cisco network environments is a combined offering that integrates BlackRidge products with Cisco ISE and Cisco DNA™ components, all engineered and validated together. The BlackRidge Enterprise Plus Security solution provides Cisco customers with additional security for cloud access, software-defined WAN connectivity and OT convergence via a single Cisco portal for policy and control. This enables the CISO and their security team to partner with the CIO and their Cisco network team to extend the organization's existing network security controls and policy management to address the risks arising from new business initiatives while maintaining visibility and control of their business environments.



Enterprise Plus Security Solution

In heterogenous environments, Cisco networks with BlackRidge Enterprise Plus Security offers customers an efficient and secure migration path, allowing them to consolidate their current security tools into a single portal through Cisco DNA. This allows Cisco customers to protect their investment in existing networking and system assets while offering future expansion opportunities through the Cisco portfolio.

Authenticate First, Connect Second!

The BlackRidge zero-trust network connection model, which authenticates identity and applies security policy before allowing network connections to be established, provides the following advantages for Cisco network environments:

- Overlays existing networks with identity-based authentication, resulting in multiple security and extensibility capabilities
- Hides and protects key business assets, applications and resources from network scanning and reconnaissance by attackers, protecting them from unauthorized awareness and access
- Extends reachability to cloud and borderless networks while protecting existing investments
- Enables visibility of authorized and unauthorized network access attempts for auditing, compliance and remediation

BlackRidge products can be deployed in a variety of network, data center and cloud configurations. Gateway software can be deployed as high-performance network appliances or as virtual appliances, and endpoint software can be installed on many different end-user devices. Deployment options include in-line as a Layer 2 transparent bridge, or logically in-line as a Layer 3 gateway.

BlackRidge products are designed to be highly resilient and can be configured for high availability and failover. Security policies can be verified during deployment with progressive installation modes of bridge, monitor and audit, and the software then enforces policy, with all actions logged to security information and event management (SIEM) systems. A management console is available to aid in deploying and maintaining a BlackRidge implementation.

About BlackRidge Technology

BlackRidge Technology enables our customers and partners to deliver more secure and resilient business services in today's rapidly evolving cyberthreat environments. The BlackRidge adaptive cyber-defense solution authenticates identity before allowing network connections, in order to proactively isolate cloud services, protect servers and IoT devices, and segment networks. Our patented technology authenticates user or device identity and enforces security policy on the first packet of a network session. This new level of real-time protection for zero trust environments blocks or redirects unidentified and unauthorized traffic to stop port scanning, cyberattacks and unauthorized access. BlackRidge was founded in 2010 to commercialize its military-grade and patented network security technologies.