BlackRidge TAC Identity Device for IoT

Secure Existing and New IT and OT Networks

Key Benefits

- **Secures IoT devices** and networks from malware and cyber-attacks via BlackRidge's patented First Packet Authentication™
- **Secures legacy environments** – adds identity-based access control with no device integration required
- **Supports regulatory compliance** and audits via identity-based network segmentation and logs of authorized connections

Information Technology (IT) and Operational Technology (OT) environments are evolving rapidly, driven by a huge influx of intelligent and connected devices – from sensors and cameras in manufacturing plants to medical devices in hospitals – that need to be protected from an increasingly complex and treacherous threat landscape. However, as the universe of connected Internet of Things (IoT) devices and applications grows, and as IT and OT environments converge, OT security has lagged, leading hackers to increasingly attack industrial control systems and Internet of Things (IoT) connected devices.

The challenge of securing industrial control systems and critical infrastructure devices can now be addressed with the BlackRidge Transport Access Control (TAC) product line. BlackRidge TAC lets organizations establish end-to-end trust by transporting identity through the stack – across already installed sensors to IoT gateways and cloud applications – both cost-effectively and with minimal latency added to the network. The BlackRidge TAC Identity Device (TAC-ID) provides identity for authenticating network connections for both new and legacy equipment in factories, hospitals and critical infrastructure architectures, and it supports the secure convergence of OT and IT networks.

The TAC-ID is ready out-of-the-box to be integrated with PTC's ThingWorx® IIoT platform and Kepware industrial automation connectivity software.

thingworx® ready

How it Works

BlackRidge secures IIoT devices and OT networks via its patented First Packet Authentication™ technology, which authenticates identity and enforces security policy on the first packet of a network session, before a connection is established. The technology blocks or redirects unidentified and unauthorized traffic, controls what authorized users or devices can access, and enables network microsegmentation and segregation of OT and IT networks.

The identity and connection authentication technologies operate at the network transport layer and can be integrated into legacy networks and virtual and cloud environments, thus allowing it to bridge the gap between existing brownfield OT infrastructure and latest-generation IT systems. The inexpensive and flexible BlackRidge TAC-ID product line creates an identity-based access control point at the IIoT device that can be physically secure and tamper evident and introduces only minimal latency into networks or manufacturing processes.

BlackRidge TECHNOLOGY

IoT Device Datasheet

Secure Legacy Environments

The hardware systems used in OT environments typically have a shelf life of a decade or longer, meaning the organizations tasked with operating and managing critical infrastructure must find a way to protect legacy equipment that is incompatible with modern network security technologies and vulnerable to today's cyber threats. BlackRidge allows organizations to start securing their OT networks today – either by installing the TAC-ID device into the network or integrating the TAC software endpoint in their current infrastructure – with minimal cost and latency impact.

BlackRidge TAC Identity Device Specifications

Product SKU	BR-4110	BR-4122
Platform Description	TAC-ID – Commercial	TAC-ID - Industrial
Trusted Port	1 x 10/100 Mbps	1 x 10/100 Mbps
Untrusted Port	1 x 10/100 Mbps	1 x 10/100 Mbps
Throughput	90 Mbps	90 Mbps
Identities	1	1
Sessions	4000	4000
Power	Micro USB	USB Type C, IEEE 802.3at PoE+
PoE Pass Through	-	IEEE 802.3at PoE+
Operating Temperature	32 to 113° F (0 to 45° C)	-40 to 185° F (-40 to 85° C)
IP Rating - Enclosure	-	IP67
Power Consumption	< 1.5 W	< 1.5 W
Dimension	2.28 x 2.28 x 1.00 in (5.8 x 5.8 x 2.5 cm)	6.34 x 4.77 x 2.48 in (16.1 x 12.1 x 6.3 cm)
Emissions	CE / FCC Class B	CE / FCC Class B

Product Deployment Options

BlackRidge products can be deployed in a variety of network, data center and cloud configurations. Our gateway software can be deployed as high-performance, network appliances or as virtual appliances, and our endpoint software can be installed on various end user devices. Deployment options include in-line as a Layer 2 transparent bridge, or logically inline 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 then enforce 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 cyber threat environments. Our zero trust approach to cyber defense uses identity to authenticate network connections and enforces identity across networks, to proactively stop cyber-attacks and protect your cloud services, servers and IoT devices.