Secure PTC ThingWorx in Cloud Environments

Addressing the Security Challenge at the Convergence of the Physical and Digital Worlds

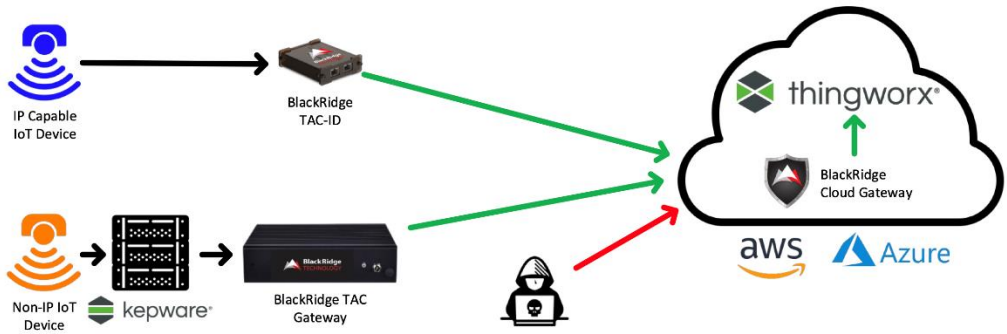
New digital services and connected industrial controls systems continue to be at high risk from security breaches and the subsequent impacts to consumer privacy and now personal safety. The challenge of securing industrial control systems (ICS) and other critical infrastructure devices and systems can 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 clouds and gateways – both cost-effectively and with minimal latency added to the network.

BlackRidge can protect the PTC ThingWorx® IoT platform in on-premises, cloud or hybrid deployments, stopping cyber-attacks and insider threats by allowing only identified and authorized users and devices to connect to the platform. As a PTC ThingWorx Ready partner, BlackRidge certified products are listed in the PTC ThingWorx Marketplace, the premier online exchange for the Industrial IoT. The PTC Partner Network accelerates solution providers and buyers' ability to capitalize on physical digital convergence by providing a broad and capable ecosystem of complementary technologies, solutions and services that accelerate their design, development, implementation and production time for their solutions.

How BlackRidge Works

To protect PTC ThingWorx in the cloud a BlackRidge cloud gateway and a BlackRidge TAC Identity Device (TAC-ID) are deployed to secure the end to end communication. PTC ThingWorx is deployed to the AWS or Azure cloud as a virtual resource. Access to PTC ThingWorx is controlled by the BlackRidge cloud gateway, which will only allow access to requests that have an authenticated identity. The identity is generated by the BlackRidge TAC-ID, which is a lightweight device that is attached to a remote device, or it can be a BlackRidge TAC endpoint integrated into an IT or IoT device. The power of the BlackRidge endpoint or TAC-ID is that the remote user or device does not need to "log in" to authenticate (something that few IoT devices do). The identity required is delivered via an X.509 v3 certificate, configured in the TAC endpoint or TAC-ID when it is deployed.

The cloud gateway intercepts incoming traffic destined for PTC ThingWorx and will only forward traffic from authorized IT and OT devices. All other traffic will be stopped and discarded by the cloud gateway, effectively making PTC ThingWorx invisible to any unauthorized entity.



IoT Device to PTC ThingWorx Authentication

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 supports the secure convergence of OT and IT networks. The TAC-ID can also provide a secure means to connect IT and OT infrastructure to development tools in the cloud, such as PTC ThingWorx. Here's how it works:

1. The IoT device is connected to the Trusted port of the TAC-ID. The Untrusted port of the TAC-ID is then connected to any network that faces the outside internet. Since the BlackRidge TAC-ID solution lives entirely on the TAC-ID device itself, no further configuration or client installation is needed on the IoT device.

2. When the IoT device initiates a connection to PTC ThingWorx in an AWS or Azure cloud, the TAC-ID, presents its authenticated identity, the pre-installed X.509 v3 certificate, to the BlackRidge cloud gateway that is protecting PTC ThingWorx. The cloud gateway compares the TAC-ID's certificate with its own database of known certificates. If there is a match, the cloud gateway creates an identity for the TAC-ID in a separate database.

3. Once an identity is created, the BlackRidge cloud gateway responds to the TAC-ID with an acceptance message and a unique "token" hash created for the identity. Now that the TAC-ID is registered with the cloud gateway, the IoT device can begin sending traffic to the PTC cloud gateway by attaching an identity token in outgoing packets.

4. Upon receiving tokenized traffic that resolves to the authorized identity, the BlackRidge cloud gateway forwards and NATS the traffic from the IoT device to PTC ThingWorx. Since all authentication exchanges happen between the TAC-ID and cloud gateway, the process is 100% transparent to both the IoT device and the PTC ThingWorx application, and it is also transparent to anyone observing the traffic.

5. Because the BlackRidge cloud gateway only responds to connection requests where it can authenticate an identity, the PTC ThingWorx application is protected from port scanning and reconnaissance. The PTC ThingWorx application is essentially cloaked and protected from and malicious traffic.

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. The BlackRidge adaptive cyber defense solution authenticates identity before allowing network connections 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 network sessions. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic to stop port scanning, cyber-attacks and unauthorized access. BlackRidge was founded in 2010 to commercialize its military grade and patented network security technologies.