REPORT REPRINT

# BlackRidge leverages authenticated identity in a zero-trust approach to securing IoT environments

**JUNE 05 2019**

**By Christian Renaud, Patrick Daly**

The company is utilizing a clever method of inserting identity tokens into the initial network connection handshake of IoT endpoints to authenticate the individual devices as the foundation of a broader device identity scheme and entitlements.



451 Research®

## Introduction

BlackRidge Technology has its roots in securing network connections in military applications, and is leveraging that expertise to build a framework of trust for IoT environments. The company utilizes a clever method of inserting identity tokens into the initial network connection handshake (TCP SYN) of IoT endpoints to authenticate the individual devices as the foundation of a broader device identity scheme and entitlements.

## 451 TAKE

BlackRidge has developed a low-friction method of building a system of identity and authentication for internet protocol (IP)-native and brownfield IoT equipment that doesn't require a rip-and-replace of devices with new ones with trusted computing or encryption chips. The legacy installed base of devices in manufacturing, transportation, healthcare and energy does not have hardware-supported authentication and assertion of identity, so BlackRidge's approach of burying a token exchange in the negotiation of a network connection should appeal to security-conscious enterprises. The security of IoT implementations continues to be the leading impediment to deploying IoT initiatives, according to respondents to 451 Research's Voice of the Enterprise, IoT surveys.

## Context

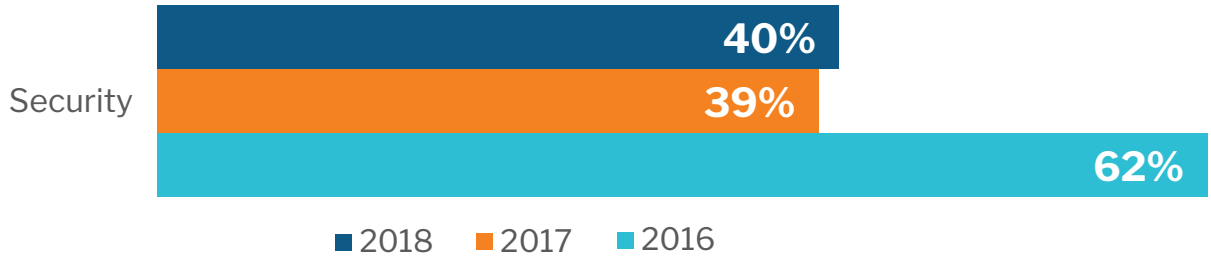
Founded in 2010, BlackRidge began as a solution for securing battlefield communications. Since many devices in combat situations are now networked, they represent an attractive target for adversaries that would wish to do reconnaissance and disrupt enemy communications. TCP/IP is highly flexible, but exposes potential security openings during the initiation of new sessions. BlackRidge embeds a unique identity token in the SYN packet of the Transmission Control Protocol (TCP) handshake, or SYN/SYN-ACK/ACK, before a layer 4 TCP/IP connection is established. The connection request is received by a BlackRidge identity gateway (a physical device or a virtual gateway in software), where the original token is authenticated and security policy entitlements are determined. Alternatively, if the token is absent or incorrect, the connecting network can decide to reject the connection, or accept the connection but forward traffic to an alternate network segment where it can be examined.

The publicly traded 50-person company is led by CEO Bob Graham and CTO and founder John Hayes, both of whom come from IT vendor and security consulting backgrounds. The market capitalization of the company at the time of this report was $19.37m. We estimate annual revenue of the company to be $5m-10m.

Security concerns continue to be the leading impediment to deploying IoT initiatives among both IT and operational technology stakeholders within enterprises, according to 451 Research's Voice of the Enterprise and Voice of the OT Stakeholder surveys. Additionally, 81% of IT respondents say that recruiting staff with skills in IoT security is moderately to very difficult. Not surprisingly, security is a top criterion for vendor partner selection among those enterprises to augment in-house staff, and the fastest-growing area of spending increases in IoT project budgets.

**Impediments to deploying IoT initiatives**

*Source: 451 Research Voice of the Enterprise, Internet of Things, Organizational Dynamics 2018*




(% of respondents 2016 n=412 / 2017 n=325 / 2018 n=385)

## Products

The BlackRidge Transport Access Control (TAC) product family consists of the individual devices attached to endpoints, the TAC Identity device (TAC-ID) and the identity gateway that validates the device identity token. The identity gateway can be either a physical device or a virtual gateway hosted in a cloud environment. The company also has near-term plans to expand the portfolio with an industrial-grade TAC-ID with anti-tamper capability and extended temperature range, as well as an embedded version of the TAC-ID on programmable logic controllers (PLCs).

BlackRidge has been granted eight patents, and has applied for seven more focused on methods of authenticating devices from the first packet and then routing traffic based on the response from the identity gateway. Unlike encryption or deep packet inspection devices, the latency of the BlackRidge technology is negligible. This is critical given the latency sensitivity of many factory and utility applications. The company monetizes its technology by taking a small fee on the activation of identity of a user or a device, and on licensing the identity gateway that performs the enforcement actions.

## Partners

Although the company sells its own 'bump on a wire' solution with the TAC-ID, the primary goal of the company is to embed its technology into partner and vendor environments. One example of a partner that is integrating with BlackRidge is National Instruments, a manufacturer of data acquisition and control systems. National Instruments is an ideal partner for smaller BlackRidge because it has a vast installed base across industries ranging from aerospace to manufacturing, many of which use the company's drag-and-drop systems engineering software, LabVIEW.

In addition to National Instruments, BlackRidge is listed in the PTC Marketplace with a solution to protect the PTC ThingWorx development platform and the Kepware IoT connectivity platform in on-premises, cloud or hybrid deployments, allowing only identified and authorized users and IoT devices to connect to the platforms. The next step in IoT partnerships for the company is to integrate closely with public cloud environments such as Microsoft Azure Sphere and AWS IoT, and with leading PLCs such as Rockwell.

## Competition

As stated previously, the current methods of securing IoT traffic come from one or more sources, including hardware root of trust, with a cryptographic key inserted in hardware at the point of manufacture; 'bump on a wire' encryption devices that encapsulate device data for transport to a location closer to where analysis occurs; and deep packet inspection (DPI). Hardware root of trust is ideal because it uniquely identifies devices; however, this requires that the device be manufactured with this capability, which is not a realistic option for legacy brownfield environments with existing industrial equipment with decades-long usage cycles.

Encryption is a key technology in all networks, and while BlackRidge is not a substitute for encryption, it complements it with identity authentication and the resulting security policy entitlements. DPI is also a critical security tool for egress traffic from a network to ensure that sensitive data is not exfiltrated within seemingly innocuous traffic.

BlackRidge is not the only vendor developing a secure identity system for IoT devices. Sectigo, formerly Comodo CA, was spun off from Comodo to focus specifically on issuing and managing IoT device certificates, and the company's recent acquisition of Icon Labs provides it with the means to filter traffic, detect unauthorized device changes and initiate secure boot. Intertrust is another vendor combining its managed certificate offering, Seacert, with application hardening based on white-box cryptography to validate device identities and secure applications in runtime. Other IoT-specific vendors in this space include Device Authority and Rubicon Labs, both of which issue and manage identities while providing broad device and policy management functionality.

## SWOT Analysis

### STRENGTHS

The technology easily integrates into greenfield and brownfield environments alike, and requires no changes to endpoints to incorporate identity of connected devices.

### WEAKNESSES

The technology addresses identity of connected devices, but does not address holistic security challenges, including encryption, behavioral analytics and deep packet inspection.

### OPPORTUNITIES

The partner integrations with National Instruments, Cisco, PTC, Rockwell and future cloud partners should increase the penetration of the TAC portfolio, inherently increasing its value in the multi-vendor IoT environment.

### THREATS

As IP-native endpoints gradually replace brownfield industrial equipment, they will incorporate hardware root-of-trust capabilities, either obviating the need entirely or requiring BlackRidge's TAC software to be integrated on those endpoints for its tokenized identity access control system to operate. This will not happen for many years, however.