REPORT REPRINT

BlackRidge Technology takes the low road to network access security

ERIC HANSELMAN

24 JUL 2018

Establishing trust with the first packet of a network connection opens interesting protection possibilities. BlackRidge is expanding from defense roots to the commercial security market with an offering that integrates identity and access control.

451 Research®

There are many ways to secure network access and manage identity. Application-level approaches usually involve an exchange of credentials and a mutual establishment of trust. Network-level approaches have more often relied on simple address identification for initial access controls and then used higher-level mechanisms to fully establish trust. BlackRidge Technology is taking an approach that embeds the ability to validate identity at the network layer, before any packet exchange has taken place. Its offering is making the leap from the battlefield to the commercial security world, and offers interesting network-protection possibilities.

THE 451 TAKE

Bringing identity validation to low-level networking protocols has an important set of advantages. It helps to make network services harder to detect, and could blunt denial-of-service attacks. BlackRidge has had success in the defense sector, and is beginning to court commercial customers. With gateways or endpoint agents required, there's some integration effort involved, but it could be attractive to those whose dedicated applications require a layer of more significant access protection.

CONTEXT

The technology behind BlackRidge's products was developed by Ridge Partners as part of a warfighter protection prototype that received funding from the US Department of Defense (DoD). BlackRidge Technology was incorporated in 2010 to put the funding to work as a joint project with the US Army. For the next few years, the company was buffeted by the ebbs and flows of DoD funding, and in 2015 it struck a deal with IBM to port the technology to the Z Mainframe environments that launched the following year. Marist College was the first commercial deployment site. The Reno, Nevada company has approximately 40 employees and, in March 2017, entered the Nasdaq OTC market through a reverse merger with Grote Molen.

TECHNOLOGY

The fundamental element to BlackRidge's technology is the ability to validate the first packet in a TCP connection before any reply is sent. It bundles identity authentication and policy enforcement into this process for a result that allows sophisticated protection of network-based services. The technology is called transport access control (TAC), and is quite different from network access control (NAC) mechanisms that security practitioners might be familiar with. With TAC, the first packet that is sent as part of a connection to a network service (the TCP SYN packet) has an encrypted token encoded into it. The receiving server authenticates the token with the BlackRidge management system before responding to the initial packet. This differs from other protection methods that require that the TCP session be established before authentication takes place.

The benefit of this technique is that network-based services don't have to reveal themselves by replying to an initial connection request. Attackers will perform extensive network reconnaissance by scanning ranges of addresses and TCP ports, looking for responses, and then attacking anything that replies in hope of gaining entry. By being able to authenticate the first packet that arrives, TAC removes the need to respond to gain an understanding of whether the traffic is legitimate or not. An additional benefit is that denial-of-service attacks (DoS, DDoS) are more complicated to achieve when the BlackRidge gateway can simply identify the first packet as invalid and discard it.

Deployment of the technology requires that TAC software be at both ends of the network conversation. This can be done by installing gateways through which traffic passes or by installing software agents in workstations and servers. The BlackRidge token has to survive the transit through network proxies and address translation, so TAC has the ability to either encode the token in the TCP sequence number or add it as a TCP header option.

Unlike full-stream encryption, the amount of computational work to run the TAC gateway is relatively light, meaning that it has the potential to scale reasonably effectively. There is authentication activity that occurs at the beginning of each connection, but subsequent packets are simply forwarded. The company says that, in 2014, a gateway demonstration passed 100Gbps of traffic. This kind of capability could be integrated into applications from ISVs that are looking at native protection techniques in high-security situations, but BlackRidge hasn't actively pursued this path.

PRODUCTS

The TAC gateway was originally packaged as an appliance, and has grown to offer virtual images for VMware and the KVM hypervisor, as well. There are cloud-hosted versions on AWS and IBM Cloud, with Microsoft Azure and Oracle Cloud slated for the fourth quarter of this year. The TAC gateway is also available as a virtualized network function that can run on Ciena's Blue Planet environment. The TAC workstation agent is available in Windows and Linux versions.

The BlackRidge management system is deployed as a virtual image. It can integrate with identity management systems and feed event streams to SIM/SIEM systems. It offers policy controls to manage where, when and how users have access to protected environments. To smooth installation, TAC software has a monitor mode that doesn't enforce access protection, but reports on actions that would have been taken. BlackRidge has built integration into security management systems from IBM (with QRadar), as well as Cisco ISE for authentication and through pxGrid for event integration.

BlackRidge has hit a number of recent milestones in product development. In March, its cryptographic module received FIPS 140-2 validation, enabling procurement by US federal government agencies and others with heightened security requirements. In June, it received certification that added it to the DoD Information Network Approved Products List. This should expand its opportunities in defense and federal markets.

COMPETITION

Network-based isolation appears in the market in a number of forms, placing potential competitors in a number of areas. On one hand, the collection of isolation technologies flying under the banner of microsegmentation will compete for mind share, although they are low-level and don't typically include identity information in their policy controls. They also require a network management and configuration capability. This would include vendors like VMware with its NSX and vArmour. Startup Edgewise Networks combines identity with application-aware controls in a more firewall-like package. A closer competitor could be Illumio, which also uses agents in server deployments. It's focused on intra-application communications and, like the others, doesn't offer resistance to network interface scanning.

The need to install gateways and agents will bring TAC into the same area as VPN providers like Juniper Networks and ScaleFT (just acquired by Okta). Although they address different markets, the waters are already muddied enough to require some work at differentiation. Those that have more significant security requirements will see these concerns as easy to overcome.

SWOT ANALYSIS

STRENGTHS

Low-level protection that can cloak the presence of network services is a powerful protection tool. Identity integration is key to providing depth in policy controls.

WEAKNESSES

Having to install gateways and agents, and the concerns around complexity that they bring, could be a deterrent to some.

OPPORTUNITIES

There's the potential for integration of the BlackRidge agent software into application stacks for ISVs that are concerned about higher levels of security.

THREATS

The information security market is crowded and complex, and the values that TAC offers could be drowned out by the din of other access technologies. Okta's recent acquisition of ScaleFT is an indication that vendors are looking at access options.