REPORT REPRINT

Barkly joins endpoint security market with approach centered on ease of use

FERNANDO MONTENEGRO

21 MAR 2018

Endpoint security has evolved constantly since the early days of antivirus. Yet amid the increased sophistication of attacks is the reality that many teams also want simplicity. Yes, effectiveness is critical but so is efficiency, both in terms of endpoint resources and operational overhead. Barkly is proposing that its multi-vector approach and SaaS offering achieves both.

451 Research®

Endpoint security is a highly competitive sector of the broader security market, contested by a number of vendors approaching the issues from different perspectives. The generational shift from time-tested antivirus approaches to more modern methods – almost always based on machine-learning techniques – is well underway, with many options for an enterprise to choose from.

Still, a number of potential customers don't fit the mold of a large enterprise and can't afford to spend the human resources needed to maintain complex endpoint products. This is the space that startup Barkly is aiming to fill – how to deliver an endpoint protection offering designed for organizations that don't want the hassle associated with policy management, complex widespread deployment and event management workflows.

THE 451 TAKE

There's great value in being able to do something quickly, efficiently, and with no fuss. For many organizations, this is what they want out of endpoint security – modern protection, easy to use and not too demanding of staff because they're busy doing things more valuable to the business. This is the segment Barkly is going for. Barkly is led by experienced executives and appears to be focused on its mission of delivering security functionality – including the by now almost mandatory machine-learning techniques – with minimal operational impact. This thinking permeates the product design, including avoiding interruptions to user workflows, or providing convenient back-end interfaces that account for remote access. As the company navigates next steps, it must account for two critical aspects. First, some improvements to Windows 10 architecture are not compatible with Barkly, so the company must address functionality in these cases. Second, the increased appetite for managed security services may also present a roadblock as providers choose alternative technologies.

CONTEXT

Barkly is a Boston-based startup, originally founded in 2013. The company has roughly 50 employees and is led by co-founders Mike Duffy (CEO) and Jack Danahy (CTO). Before founding Barkly, Duffy led OpenPages, a GRC vendor that was acquired by IBM in 2010. His earlier career included executive roles at Intel, Shiva Corp and GTE. Jack Danahy was previously founder and CEO of Qiave Technologies (acquired by WatchGuard in 2000) and Ounce Labs (acquired by IBM in 2009). Prior to Barkly, Danahy was a director at IBM.

The company has raised $23.5m in seed and A rounds, with investments from New Enterprise Associates and Sigma Prime Ventures. Its latest raise was $6m in Jan 2017. The company indicated it has been shipping its product since mid-2017 and has about 100 customers. 451 Research estimates its revenue to be in the $300,000-1m range.

PRODUCTS

Barkly's offering is named Endpoint Protection Platform, and consists of three main functions: ProtectIQ, which is the core protection functionality, implemented through a local agent on the endpoint; EvolveIQ, a centralized, cloud-based analytics pipeline for machine learning hosted on AWS; and CommandIQ, the back-end management portal.

The product is aimed at midmarket organizations, typically those struggling to protect themselves against modern attacks but have limited security resources on staff. The product aims to provide protection against traditional as well as newer threats, such as fileless and exploit-based campaigns. While there is some support for EDR-like queries and responses, Barkly has focused on protection against attacks. The target use case is focusing on improving preventative actions rather than elaborate forensic investigations. The product is compatible with and complementary to existing antivirus products, although it may also be used as a replacement for them.

Barkly uses a combination of machine-learning and behavioral heuristics (rules) to inspect and determine the threat associated with executing known and unknown binaries. It also analyzes scripts, which are often associated with fileless attacks. The core analysis that Barkly performs is done by observing machine instructions that are indicative of malicious behavior, rather than pinpointing specific threats. The protection is implemented fully on the agent, removing the need to have a constant connection to the cloud-based service. The local agent, Rapidvisor, uses a multi-tiered approach to monitoring local systems and is supported on Windows 7 and above, as well as Windows Server 2008 and above. The agent itself is lightweight, typically consuming less than 1% of CPU resources.

The agent can be distributed using traditional software distribution methods and does not require a reboot for installation. Protection functionality is provided by combining input from three distinct layers: user space monitoring, focused on detecting malicious scripts and malware via Barkly's machine learning predictors; kernel-mode drivers, tackling, among other things, malicious process injection, process impersonation and credential theft; and a proprietary type I hypervisor that implements CPU and kernel integrity enforcement controls, including hardware-enabled system call interception, and support for enforcement of Supervisor Mode Execution Prevention and Supervisor Mode Access Prevention features. The hypervisor module is not compatible with Microsoft's Hyper-V virtualization, but nests within other common virtualization platforms.

Barkly's machine-learning pipeline is implemented under the EvolveIQ moniker. It executes centrally from Barkly-managed AWS infrastructure, with models pushed down to endpoints periodically as directed by automated testing and accuracy assessment modules. EvolveIQ uses both supervised and unsupervised approaches. Supervised machine learning is used to help identify malware. The company uses training data that includes malware samples from several locations, as well as 'goodware': structural information about valid, benign applications, derived from agent prediction activity on each customer deployment.

As a result, when choosing a model to push to the endpoints, Barkly can use either a model trained on a broad set of good software, or a model tailored to each specific customer by training against their specific software profile. The company also uses unsupervised machine learning within its research group as it analyzes behavior sequences, generating clusters or families of similar attacks. This is used in development of behavioral rules that can then capture future attacks that are functionally similar to those already analyzed.

Last, Barkly's centralized management capabilities – named CommandIQ – support alerting and reporting, automatic agent upgrades, incident forensics and response, and SIEM integration. The company focused heavily on simplifying operations for its target customers, and the back-end interface includes simplified actions for alerts and provides broad support for access from mobile devices.

STRATEGY

The company is very clear in that it is targeting midmarket organizations, which it sees as underserved. It views many advanced security vendors as focusing on larger enterprise use cases, and overlooking the protection needs of organizations that have not invested in larger and more experienced security teams.

Barkly highlights that in addition to being compatible with and complementary to existing antivirus products, its offering can stand alone as a replacement. The company has obtained favorable third-party evaluations of the Barkly platform under the requirements of PCI-DSS 3.2, NIST and the HIPAA Security Rule.

Barkly has focused on North America and English-speaking countries. The company is building out its channel partnerships selectively. Barkly has indicated that it's aware of the need to work alongside managed security service providers because they represent a key vehicle for delivering security services to midmarket customers.

COMPETITION

Competition in the endpoint space is fierce and is fought in terms of technology as well as mindshare. As Barkly goes to market targeting the midmarket and smaller enterprise space, it faces vendors from several angles.

Traditional endpoint security vendors – Symantec, McAfee, Trend Micro, Sophos, Kaspersky – have significant 'mindshare' and well-oiled channels that reach into the midmarket. While their offerings tend to be more enterprise-focused, their ongoing effort to simplify delivery means they can likely compete in smaller accounts as well.

The midmarket space is also contested by vendors with a strong history in SMB or more niche roles in enterprise. The list includes vendors such as Bitdefender, Malwarebytes, Panda Security, and ESET, to name a few. More recent entrants, such as Carbon Black, Cylance, SentinelOne and Endgame also represent competition. Many of these vendors have been focusing on simplifying operations and, given their broad market presence, are also on potential customers' radar.

Barkly's target customer is also a strong candidate for adopting managed services, either as managed desktops or managed security services. The list of possible providers is immense, ranging from established vendors such as Red Canary and SecureWorks to many smaller offerings from integrators and local resellers. From a technology angle, many of these offerings rely on vendors such as Carbon Black, CrowdStrike, enSilo and Secdo.

Last, there is also possibility of competition from the natural evolution of the operating system itself. Microsoft has made several additions to its flagship Windows 10 product. Customers that are comfortable with Microsoft's ecosystem may choose to go that route.

SWOT ANALYSIS

STRENGTHS

Barkly's different layers of protection with the agent, combined with the simplicity of managing the overall deployment, make a compelling case for organizations looking for an approach to endpoint security with low operational impact.

WEAKNESSES

The current lack of a MacOS agent may be an issue in some customer environments. The company needs to ensure consistent levels of protection in environments leveraging Windows 10 virtualization-based security features, which are incompatible with the Barkly hypervisor.

OPPORTUNITIES

Customers are looking at the evolution of endpoint security and open to considering alternative vendors. The target customer profile for Barkly is likely to appreciate a no-hassle approach.

THREATS

In addition to fierce competition from endpoint security vendors, the changing nature of the endpoint operating system itself poses a threat, as Microsoft adds increased security functionality of its own. The customer segments favored by Barkly are also ripe for considering managed security services that may leverage alternate vendors.